CHALMERS

GÖTEBORGS UNIVERSITET

Expandergrafer

Spektral grafteori och felrättande koder

Kandidatarbete inom civilingenjörsutbildningen vid Chalmers

Christian Al-Maleh
Stefan Areback
Andreas Dahlberg
Johan Gustafsson
Tomas Pousette

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2018

Expandergrafer

Spektral grafteori och felrättande koder

Kandidatarbete i matematik inom civilingenjörsprogrammet Teknisk fysik vid Chalmers
Tomas Pousette

Kandidatarbete i matematik inom civilingenjörsprogrammet Teknisk matematik vid Chalmers
Christian Al-Maleh Stefan Areback Andreas Dahlberg Johan Gustafsson

Handledare: Michael Björklund
Examinatorer: Maria Roginskaya och Marina Axelson-Fisk

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2018

Populärvetenskaplig presentation

Det är känt att varje ändlig graf i $\mathbb{R}^3$ kan ritas utan att kanterna korsar varandra. På 1960-talet undersökte Kolmogorov och Barzdin [1] i hur liten volym en sådan graf kan existera. Detta är intressant ur ett datavetenskapligt perspektiv, nämligen att konstruera ett nätverk i en så liten volym som möjligt. Kolmogorov och Barzdin visade, genom att explicit konstruera en sådan graf, att varje 3-reguljär graf med n noder får plats i en sfär med radie ungefär $\sqrt{n}$. En naturlig fråga att ställa sig är om detta är den minsta möjliga volymen. För att svara på denna fråga definierade de en variant av det som idag kallas *expandergrafer* och lyckades därefter visa att en sfär med radie $\sqrt{n}$ faktiskt är den minsta möjliga volymen. Namnet expandergrafer myntades dock först av Pinsker, som studerade dessa under samma period [2].

Expandergrafer kännetecknas av att de har få kanter, är väldigt sammanhängande och att den kortaste vägen mellan två noder är liten i förhållande till antalet noder i grafen. Det innebär att om en eller ett par kanter tas bort från grafen så är den fortfarande sammanhängande. En praktisk tillämpning av sådana grafer kan vara att bygga broar mellan en mängd öar. I ett sådant scenario vill man ha så få broar som möjligt där det fortfarande ska vara möjligt att ta sig från en ö till en annan trots att några, slumpvist valda, broar har havererat.

Kraven att grafen ska ha få kanter och samtidigt vara mycket sammanhängande är motstridiga, vilket gör att det inte är uppenbart att sådana grafer existerar överhuvudtaget. Med hjälp av sannolikhetsteori är det möjligt att visa att för vissa *bipartita grafer* är andelen expandergrafer mycket stor. Det visar sig faktiskt att sannolikheten att en sådan graf inte är en expandergraf går mot 0 då antalet noder ökar. Detta resultat ger dock ingen explicit konstruktion av en expandergraf, vilket man är intresserad av i praktiska sammanhang. År 1973 gav Margulis ett exempel på en explicit konstruktion av en 8-reguljär expandergraf [3]. Sedan dess har andra metoder utvecklats för att konstruera expandergrafer, men dessa kräver mer avancerad matematik.

De matematiska metoder som används för att studera expandergrafer kan också användas för att studera *grupper*, genom att betrakta en så kallad *Cayleygraf* som konstrueras utifrån en grupp och en symmetrisk delmängd av denna. Till exempel kan man visa att Cayleygrafen av gruppen $SL_2(\mathbb{F}_p)$ för en tillräckligt stor symmetrisk delmängd har *diameter* som mest tre. Detta innebär att varje nod ligger högst tre kanter från varje annan nod.

Vidare har expandergrafer tillämpningar inom datalogi, till exempel vid konstruktion av *felrättande koder*. En felrättande kod är en metod för att återställa korrumperad data till sitt ursprungliga skick. Korrumpering av data kan ske på grund av brus eller fysisk degradering och är vanligt vid datalagring och dataöverföring. Detta gör idag felrättande koder till ett viktigt begrepp.

Claude Shannon och Richard Hamming anses vara pionjärerna bakom felrättande koder på grund av deras banbrytande arbete inom informationsteori runt år 1950. Detta arbete lade grunden för all den teori som ligger bakom de koder som används inom felrättning idag. Robert G. Gallager var den som började att titta på koder i termer av grafer, men begränsade sig till glesa, slumpmässiga grafer. Denna klass av koder kallas för *LDPC-koder* där akronymen står för *low-density parity check*. Dessa koder var på sin tid opraktiska att använda, men har på sistone visat sig konkurrenskraftiga. Då glesa, slumpmässiga grafer, med hög sannolikhet, är expandergrafer insåg Daniel Spielman att denna egenskap kunde användas för att analysera kodernas prestation [4]. Denna typ av grafer kom att kallas *expanderkoder* och deras forskning visade särskiljande egenskaper som att de däribland kunde rätta fel på linjär tid [5].

Sammanfattning

Först bevisas existensen av expandergrafer med Margulis konstruktion och de spektrala egenskaperna hos Markovoperatorn. Därefter visas att egenrummen till Markovoperatorn definierad på en Cayleygraf av $SL(2, \mathbb{F}_p)$ har stor dimension, vilket används för att bevisa Gowers sats för $SL(2, \mathbb{F}_p)$. Slutligen studeras bipartita expandergrafer i samband med felrättande koder, och de visas ge upphov till avkodningsalgoritmer med linjär tidskomplexitet.

Abstract

First, the existence of expander graphs is proved using Margulis construction and the spectral properties of the Markov operator. Second, the Markov operator defined on a Cayley graph of $SL(2, \mathbb{F}_p)$ is shown to have large eigenspaces, which is then used to prove Gowers theorem for $SL(2, \mathbb{F}_p)$. Finally, bipartite expander graphs are studied in the context of error correcting codes, and are shown to provide linear time decoding algorithms.

Innehåll

Förord

Under kandidatarbetets gång har en gruppdagbok samt individuella tidsloggar förts. Gruppdagboken är skriven i kronologisk ordning och beskriver i detalj de olika arbetsfaserna i kandidatarbetet. Den innehåller även de olika beslut vi valt att ta samt reflektioner kring dessa. De individuella tidsloggarna anger mer specifikt antalet timmar en viss författare ägnat åt en aktivitet.

Nedan presenteras de huvudsakliga författarna för de olika avsnitten i rapporten. Samtliga författare har dock, mer eller mindre, bidragit till alla avsnitt.

Kapitel 2:

- **Grafteori:** Christian
- **Valens, expansion och exempel på dessa:** Johan

Kapitel 3:

- **Definition av expandergrafer:** Johan
- **Spektral expansion:** Stefan

Kapitel 4:

- **Fram till och med Ekvation** (9)**:** Andreas
- **Resterande:** Tomas

Kapitel 5:

- **Inledning:** Andreas
- **Frobenius sats:** Andreas och Stefan
- **Lemma 5.3:** Stefan
- **Lemma 5.4 och Gowers sats:** Tomas

Kapitel 6:

- **Lemma 6.18:** Andreas
- **Inledning, grundläggande informationsteori, linjära koder:** Christian
- **Inledning, grundläggande informationsteori, expanderkoder:** Johan

Bilaga A:

- **Hela kapitlet:** Stefan

Bilaga B:

- **Definition B.1 och Lemma B.3:** Tomas
- **Definition B.2 och avslutande observation:** Stefan

Bilaga C:

- **Fram till och med Proposition C.2:** Andreas
- **Resterande:** Tomas

Bilaga D:

- **Hela kapitlet:** Andreas

Bilaga E:

- **Fram till och med Ekvation** (32)**:** Tomas
- **Resterande:** Andreas

1 Inledning

En expandergraf är en familj av grafer som uppfyller vissa restriktiva villkor. Dessa villkor ger graferna i familjen två motstridiga egenskaper: de är glesa men samtidigt väldigt sammanhängande. Egenskaperna gör expandergrafer användbara i både teoretiska och praktiska tillämpningar. I en första bemötelse är det dock svårt att hitta ett exempel på en graf som satisfierar de restriktiva villkoren som definierar expandergrafer. Den första delen av denna litteraturstudie är därför ämnad åt att bevisa att expandergrafer faktiskt existerar. Därefter kommer vi att studera expansion i grupper, och till sist används expandergrafer för att konstruera felrättande koder.

Både Kapitel 2 och Kapitel 3 bygger på [4]. I Kapitel 2 ges grundläggande definitioner och resultat inom grafteori. Därefter ges i Kapitel 3 definitionen av en expandergraf. Det visar sig då att svårigheten i att konstruera en expandergraf är att dess expansionkonstant måste vara strikt större än noll då antalet noder i grafen går mot oändligheten. Resterande del av Kapitel 3 ägnar sig därför åt att studera kopplingen mellan expansionskonstanten och det minsta nollskiljda egenvärdet λ_1 till den linjära operatorn $I - M$, där M betecknar Markovoperatorn, i syfte att begränsa expansionskonstanten underifrån. Den undre begränsningen lägger sedan grunden för beviset av att expandergrafer existerar, som ges i Kapitel 4 och baseras på [3]. Beviset använder sig av Margulis konstruktion, vilket är en speciell graf på vilken λ_1 är strikt större än noll. Tillsammans med den undre begränsningen visas att grafens expansionskonstant är strikt större än noll, och att grafen därmed är en expandergraf.

Egenvärdena till Markovoperatorn har även stor betydelse när det kommer till expansion av delmängder i grupper. I Kapitel 5 följer vi [6] och bevisar Gowers sats. Denna säger att om en symmetrisk delmängd A till gruppen $G = SL(2, \mathbb{F}_p)$ är tillräckligt stor så kommer dess trippelprodukt, det vill säga mängden av alla produkter abc där $a, b, c \in A$, att bli hela gruppen. Detta gör vi genom att visa att egenrummen till Markovoperatorn är representationer av G. Med hjälp av Frobenius sats kan vi då säga att egenrummen har hög dimension och därefter att egenvärdena $\lambda \neq 1$ till Markovoperatorn är väldigt små. Detta är nyckelidén i beviset av Gowers sats. Motiveringen till att studera detta problem är att det finns grupper, till exempel $\mathbb{Z}/2k\mathbb{Z}$, som har stora delmängder vars produkter aldrig kan bli hela gruppen. En följd av Gowers sats är att diametern till Cayleygrafen $\Gamma(G, A)$ är som mest 3.

Avslutningvis återkommer vi till expandergrafer i Kapitel 6 i samband med felrättande koder. Kapitlet inleds med grundläggande informationsteori som är gemensam för samtliga koder. Därefter definierar vi en särskild klass av koder, så kallade linjära koder. Vi studerar sedan de linjära kodernas paritetsmatriser i termer av grafer för att skapa koder. Om dessa grafer är expandergrafer med bra nog expansion, kan vi sedan visa att dessa koder har ett stort avstånd och en avkodningsalgoritm som kan avkoda på linjär tid. Denna analys grundas på materialet i [3].

2 Grafteori

I detta kapitel definierar vi och ger exempel på de mest grundläggande begreppen inom grafteori. Det ska ge oss en bra förståelse för de koncept som introduceras i kommande kapitel, varvid expandergrafer bland annat definieras.

Definition 2.1. (Graf) En graf $\Gamma = (V, E, \text{ep})$ ges av två mängder V och E, som motsvarar en nod- respektive kantmängd, och en *ändpunktsavbildning*

$$\text{ep} : E \longrightarrow V^{(2)} \tag{1}$$

där $V^{(2)}$ är mängden av alla delmängder av V med kardinalitet 1 eller 2.

Med denna definition studerar vi endast oriktade grafer. För riktade grafer behövs en annan definition som skiljer mellan start- och slutnoden för varje kant.

Ändpunktsavbildningen beskriver specifika noder i V som kopplas samman av en given kant. Exempelvis, om $\alpha \in E$ så består $\text{ep}(\alpha)$ av de noder som är ändpunkter till α. Om det existerar två distinkta kanter α och β så är de *angränsande* i något $x \in V$ om $x \in \text{ep}(\alpha) \cap \text{ep}(\beta)$.

En viktig egenskap hos en graf är dess *valens*. Antalet kanter i Γ för vilka en nod $x \in V$ utgör en ändpunkt kallas för valensen, eller *graden* av x, och skrivs $val(x)$ eller $deg(x)$. En graf där graden är lika för alla noder kallas för *reguljär*, eller *d-reguljär* för graden $d \geq 0$. Nedan ges två exempel på reguljära grafer, följt av ett exempel på en icke-reguljär graf.

Exempel 2.2. (Cyklisk graf) Låt $m \geq 1$ vara ett heltal. För en *m-cyklisk graf* C_m är nodmängden $V_m = \mathbb{Z}/m\mathbb{Z}$, kantmängden $E_m = \mathbb{Z}/m\mathbb{Z}$ och ändpunktsavbildningen $\text{ep}(i) = \{i, i+1\}$ där $i \in \mathbb{Z}/m\mathbb{Z}$. För varje nod $i \in V_m$, då $m \geq 2$, ser vi att precis två kanter är angränsande. Det betyder att valensen av varje nod är 2 och därmed att grafen är 2-reguljär. Om $m = 1$ består motsvarande graf endast av en nod med en kant som går från noden till sig själv. I det fallet är grafen 1-reguljär.

Exempel 2.3. (Komplett graf) Låt $m \geq 1$ vara ett heltal. För den *kompletta grafen* K_m är $V_m = \{1, \dots, m\}$, $E_m = \{(x, y) \mid x < y,\ x, y \in V_m\}$ och $\text{ep}((x, y)) = \{x, y\}$. Mellan varje par av noder finns det alltså exakt en kant. Detta betyder att valensen av varje nod är $m - 1$ och därmed att K_m är $m - 1$-reguljär.

Exempel 2.4. (Stig) Låt $m \geq 0$ vara ett heltal. För en *stig* P_m av längd m är nodmängden $V_m = \{0, \dots, m\}$, kantmängden $E_m = \{1, \dots, m\}$ och ändpunktsavbildningen $\text{ep}(i) = \{i-1, i\}$ där $1 \leq i \leq m$. En stig är alltså lik en cyklisk graf, men mellan den första och den sista noden saknas en kant. Så den första och sista noden har alltid valens 1, medan övriga noder har valens 2. Den cykliska grafen är alltså reguljär för $m = 0$ och $m = 1$, och icke-reguljär för $m \geq 2$.

Mellan varje par av noder i en graf finns det ett naturligt sätt att säga vad avståndet mellan de är. Detta gör också att vi kan definiera *diametern* av en graf. Denna anger hur nära noderna i en graf är varandra.

Definition 2.5. (Distans) Låt $\Gamma = (V, E, \text{ep})$ vara en graf. För alla $x,\ y \in V$ ges distansen mellan $x,\ y$ i Γ antingen av längden av den minsta möjliga stigen mellan dessa två noder, givet att en sådan stig existerar, annars $+\infty$. Beteckningen för distans är $d_\Gamma(x, y)$ och definieras som

$$d_\Gamma(x, y) = \min\{l(\gamma) \mid \gamma \textit{ är en stig mellan } x \textit{ och } y\} \in \{0, 1, 2, \dots\} \cup \{+\infty\} \tag{2}$$

där $l(\gamma)$ är längden av stigen γ. En graf är *sammanhängande* om och endast om $d_\Gamma(x, y)$ är ändlig för alla $x,\ y \in V$. Alltså, det finns minst en stig mellan varje par av noder.

Definition 2.6. (Diameter) Låt $\Gamma = (V, E, \text{ep})$ vara en graf. Dess diameter beskrivs som den längsta distansen mellan två noder i Γ och betecknas

$$\text{diam}(\Gamma) = \sup_{x,y \in V} d_\Gamma(x, y). \tag{3}$$

Grannmatrisen för en graf Γ är ett sätt att representera grafen. Denna ger en överblickande bild av grafen och kan användas då man vill bestämma antalet stigar mellan två noder.

Definition 2.7. (Grannmatris) Låt $\Gamma = (V, E, \text{ep})$ vara en ändlig graf. Matrisen $A_\Gamma(a(x,y))$ kallas för *grannmatrisen*, där V indexerar både raderna och kolumnerna i A_Γ och $a(x,y)$ anger antalet kanter mellan noderna x, $y \in V$,

$$a(x,y) = \left|\{\alpha \in E \mid \text{ep}(\alpha) = \{x,y\}\}\right|. \tag{4}$$

Grannmatrisen är symmetrisk, vilket anspelar på att kanternas riktning kan omvändas. Med detta i åtanke kännetecknar vi dessa kanter som *icke-orienterade*.

Definition 2.8 (Cheegerkonstanten)**.** Låt $\Gamma = (V, E, \text{ep})$ vara en ändlig graf. Mängden av kanter som går mellan två disjunkta delmängder av noder $V_1, V_2 \subset V$ skrivs

$$\mathcal{E}(V_1, V_2) = \{\alpha \in E \mid \text{ep}(\alpha) \cap V_1 \neq \emptyset, \text{ep}(\alpha) \cap V_2 \neq \emptyset\}.$$

Då endast en delmängd specificeras tas den andra delmängden att vara komplementet, $\mathcal{E}(V_1) = \mathcal{E}(V_1, V \setminus V_1)$, alltså resten av noderna. Cheegerkonstanten $h(\Gamma)$ definieras då som

$$h(\Gamma) = \min\left\{\frac{|\mathcal{E}(W)|}{|W|} \mid \emptyset \neq W \subset V, |W| \leq \frac{1}{2}|\Gamma|\right\}.$$

Ibland kallas Cheegerkonstanten även för grafens expansionskonstant. Vi noterar att kvoterna i mängden, och därmed Cheegerkonstanten, är ickenegativa. Denna är noll om och endast om grafen inte är sammanhängande.

Exempel 2.9 (Cheegerkonstanten för cykliska grafer)**.** Det gäller att $|\mathcal{E}(W)| = 2$ för varje val av C_m där $m \geq 2$. För jämna val av m kommer $|W|$ vara högst $\frac{m}{2}$ och för udda val $\frac{m-1}{2}$. Detta ger $h(C_m) = \frac{4}{m}$ respektive $h(C_m) = \frac{4}{m-1}$.

Exempel 2.10 (Cheegerkonstanten för kompletta grafer)**.** Tack vare symmetri kan vi välja en godtycklig delmängd av storlek j. Vi får då följande uttryck för Cheegerkonstanten,

$$h(K_m) = \min_{1 \leq j \leq \frac{m}{2}} \frac{1}{j}|\mathcal{E}(\{1, \ldots, j\})|.$$

Varje nod i denna mängd har $m-j$ kanter kopplade till dess komplement. Totalt blir antalet kanter $j(m-j)$ och vi får

$$h(K_m) = \min_{1 \leq j \leq \frac{m}{2}} m - j = m - \left\lfloor \frac{m}{2} \right\rfloor.$$

Definition 2.11 (Nodexpansion)**.** Mängden av alla noder i W^c som går att nå ifrån W med endast ett steg skrivs

$$\partial W = \{x \in V \mid x \notin W, d_\Gamma(x,y) = 1 \text{ för något } y \in W\}.$$

Vi kan nu införa en alternativ definition av Cheegerkonstanten,

$$\tilde{h}(\Gamma) = \min\left\{\frac{|\partial W|}{|W|} \mid \emptyset \neq W \subset V, |W| \leq \frac{1}{2}|\Gamma|\right\}.$$

Denna definition tar inte hänsyn till att flera noder i W kan ha en kant till samma nod i W^c. Nedanstående lemma visar dock att det finns en koppling mellan $\tilde{h}(\Gamma)$ och $h(\Gamma)$.

Lemma 2.12. *Låt $\Gamma = (V, E, \text{ep})$ vara en ändlig, icke-tom graf med uppåt begränsad valens v. För en godtycklig delmängd $W \subset V$ gäller*

$$\frac{1}{v}|\mathcal{E}(W)| \leq |\partial W| \leq |\mathcal{E}(W)|.$$

Bevis. Den högra olikheten följer direkt av att flera noder i W kan ha en kant till en och samma nod i W^c. Den vänstra olikheten följer av att för varje nod i ∂W så är antalet kanter som ifrån denna går in i W som mest v. □

3 Expandergrafer

I detta avsnitt kommer vi definiera vad en expandergraf är och därefter presentera och bevisa en sats som är väldigt användbar då man vill bevisa att en familj av grafer är expandergrafer.

Definition 3.1 (Expandergrafer)**.** En familj $(\Gamma_i)_{i\in I}$ av ändliga, icke-tomma, sammanhängande grafer sägs vara en familj av expandergrafer om det finns konstanter $v \geq 1$ och $h > 0$ så att

$$\max_{x\in V_i} \mathrm{val}(x) \leq v$$
$$h(\Gamma_i) \geq h > 0$$

där det finns ett ändligt antal $i \in I$ så att $|V_i|$ är som mest N för alla $N \geq 1$.

Den intuitiva tolkningen av ovanstående definition är att (Γ_i) är expandergrafer om graferna i familjen ökar i storlek samtidigt som gradtalet är begränsat och Cheegerkonstanten håller sig borta från noll. Vi noterar också att (Γ_i) måste vara oändligt stor, för om familjen endast innehåller ändligt många sammanhängande grafer med begränsat gradtal kan man sätta h till den minsta av grafernas Cheegerkonstant och v till det största gradtalet och få en expanderfamilj. Från exemplen i förra kapitlet kan vi se att den cykliska grafen är väldigt gles, men inte starkt nog sammankopplad. För den kompletta grafen har vi istället att denna graf är väldigt väl sammankopplad, men inte gles nog för att uppfylla kriteriet för expandergrafer.

När det kommer till expandergrafer så kvittar det om man definierar Cheegerkonstanten som (2.8) eller (2.11). Det vill säga, om en graf är en expandergraf enligt den ena definitionen så är den även en expandergraf enligt den andra och vice versa. Detta följer enkelt av Lemma (2.12).

Vi kommer nu bevisa att för att bestämma huruvida en familj grafer är en expanderfamilj kan man titta på det minsta nollskiljda egenvärdet till en linjär operator $I - M$, som vi betecknar med $\lambda_1(\Gamma)$ (nedan kommer vi visa att alla egenvärden till denna operatorn är reella, så vi kan tala om det minsta egenvärdet till denna operator). Detta kriterium kommer att användas i Margulis konstruktion av en familj av expandergrafer i kapitel 4. Operatorn I är identitetsoperatorn på vektorrummet $L^2(\Gamma) = \{f : V_\Gamma \longrightarrow \mathbf{C}\}$ och M är *Markovoperatorn*, som vi definerar nedan. Mer precist har vi följande sats.

Sats 3.2. *En familj $(\Gamma_i)_{i\in I}$ av ändliga sammanhängande grafer är en expanderfamilj om antalet noder går mot oändligheten och det finns konstanter $v \geq 1$ och $\lambda > 0$ så att $\max_{x\in V_{\Gamma_i}} \deg(x) \leq v$ och $\lambda_1(\Gamma_i) \geq \lambda$ gäller för alla $i \in I$.*

Denna sats följer omedelbart från följande sats, som vi kommer att bevisa nedan.

Sats 3.3. *Antag att Γ är en ändlig sammanhängande graf. Då gäller*

$$\lambda_1(\Gamma) \leq \frac{2v_+}{(v_-)^2} h(\Gamma),$$

där $v_+ = \max_{x\in V_\Gamma} \deg(x)$ och $v_- = \min_{x\in V_\Gamma} \deg(x)$.

I resten av detta avsnittet kommer vi anta att Γ är ändlig och sammanhängande. Markovoperatorn $M : L^2(\Gamma) \longrightarrow L^2(\Gamma)$ definieras genom

$$M\varphi(x) = \frac{1}{\deg(x)} \sum_{y\in V_\Gamma} a(x,y)\varphi(y), \tag{5}$$

för $\varphi \in L^2(\Gamma)$, där $a(x,y)$ är elementen i grannmatrisen. Detta är en linjär operator på $L^2(\Gamma)$. Vi definierar en inre produkt på $L^2(\Gamma)$ genom

$$\langle \varphi, \psi \rangle = \frac{1}{N} \sum_{x\in V_\Gamma} \varphi(x)\overline{\psi(x)} \deg(x), \tag{6}$$

där $N = \sum_{x \in V_\Gamma} \deg(x)$. Med avseende på denna inre produkten är M en självadjungerad operator. För om $\varphi, \psi \in L^2(\Gamma)$ så har vi

$$\begin{aligned}
\langle M\varphi, \psi \rangle &= \frac{1}{N} \sum_{x \in V_\Gamma} M\varphi(x)\overline{\psi(x)} \deg(x) \\
&= \frac{1}{N} \sum_{x \in V_\Gamma} \Big(\frac{1}{\deg(x)} \sum_{y \in V_\Gamma} a(x,y)\varphi(y) \Big) \overline{\psi(x)} \deg(x) \\
&= \frac{1}{N} \sum_{y \in V_\Gamma} \varphi(y) \Big(\overline{\frac{1}{\deg(y)} \sum_{x \in V_\Gamma} a(y,x)\psi(x)} \Big) \deg(y) \\
&= \langle \varphi, M\psi \rangle.
\end{aligned}$$

Vi kommer också behöva följande egenskap hos M.

Sats 3.4. *Egenrummet till M hörande till egenvärdet 1 består av alla konstanta funktioner på Γ.*

Bevis. Att en konstant funktion är en egenvektor med egenvärde 1 följer direkt från definitionen av M, om man noterar att $\deg(x) = \sum_{y \in V_\Gamma} a(x,y)$. Anta nu att $\varphi \in L^2(\Gamma)$ är en egenvektor hörande till egenvärdet 1, det vill säga $M\varphi(x) = \varphi(x)$ för alla $x \in V_\Gamma$. Om φ inte är en konstant funktion så finns en nod x_0 så att $\varphi(x_0) = \min_{x \in V_\Gamma} \varphi(x)$ och så att x_0 har en granne y_0 så att $\varphi(y_0) > \varphi(x_0)$ (här använder vi att Γ är ändlig och sammanhängande). Då har vi

$$\begin{aligned}
\varphi(x_0) &= \frac{1}{\deg(x_0)} \sum_{y \in V_\Gamma} a(x_0, y)\varphi(y) \\
&\geq \frac{1}{\deg(x_0)} \big(\varphi(x_0)(\deg(x_0) - 1) + \varphi(y_0) \big).
\end{aligned}$$

Denna olikheten är ekvivalent med olikheten $\varphi(x_0) \geq \varphi(y_0)$, vilket motsäger antagandet $\varphi(y_0) > \varphi(x_0)$. Alltså måste φ vara en konstant funktion. □

Eftersom både I och M är självadjungerande operatorer på $L^2(\Gamma)$ är även $I - M$ en självadjungerande operator på $L^2(\Gamma)$. Eftersom 1 är ett egenvärde till M vars egenrum består av alla konstanta funktioner på Γ, så är 0 ett egenvärde till $I - M$ med samma egenrum. Eftersom $I - M$ är självadjungerande ligger alla egenvektorer till $I - M$ hörande till egenvärden skiljda från 0 i det ortogonala komplementet till delrummet av $L^2(\Gamma)$ bestående av konstanta funktioner. Begränsar vi $I - M$ till att verka på detta delrum får vi en ny självadjungerad operator, vars minsta egenvärde är lika med $\lambda_1(\Gamma)$. Med hjälp av Sats (A.11) får vi en formel för $\lambda_1(\Gamma)$ som låter oss relatera denna siffra till Cheegerkonstanten för Γ:

$$\lambda_1(\Gamma) = \min_{0 \neq \varphi \perp 1} \frac{\langle (I - M)\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle}.$$

Lemma 3.5. *För alla $\varphi \in L^2(\Gamma)$ gäller*

$$\langle (I - M)\varphi, \varphi \rangle = \frac{1}{2N} \sum_{x,y \in V_\Gamma} a(x,y)|\varphi(x) - \varphi(y)|^2. \tag{7}$$

Bevis. Vi har $|\varphi(x) - \varphi(y)|^2 = |\varphi(x)|^2 + |\varphi(y)|^2 - \overline{\varphi(x)}\varphi(y) - \varphi(x)\overline{\varphi(y)}$. Från detta och

$$\frac{1}{2N} \sum_{x,y \in V_\Gamma} a(x,y)|\varphi(x)|^2 = \frac{1}{2N} \sum_{x \in V_\Gamma} |\varphi(x)|^2 \deg(x) = \frac{1}{2}||\varphi||^2$$

och

$$\begin{aligned}
&\frac{1}{2N} \sum_{x,y \in V_\Gamma} a(x,y)\varphi(x)\overline{\varphi(y)} \\
&= \frac{1}{2N} \sum_{y \in V_\Gamma} \Big(\frac{1}{\deg(y)} \sum_{x \in V_\Gamma} a(x,y)\varphi(x) \Big) \overline{\varphi(y)} \deg(y) = \frac{1}{2}\langle M\varphi, \varphi \rangle
\end{aligned}$$

följer formeln. □

Definition 3.6. Låt S vara en mängd och T en delmängd av S. Den karaktäristiska funktionen av T definieras som

$$\chi_T(x) = \begin{cases} 1, & \text{om } x \in T \\ 0, & \text{annars,} \end{cases}$$

för $x \in S$.

Det enda vi behöver nu för att bevisa Sats 3.3 är följande två hjälpsatser.

Lemma 3.7. *Låt $W \subseteq V_\Gamma$ och definiera $\varphi_W = \chi_W - \langle 1, \chi_W \rangle$. Då gäller*

$$\langle (I - M)\varphi_W, \varphi_W \rangle = \frac{|\mathcal{E}(W)|}{N},$$

och

$$\langle \varphi_W, \varphi_W \rangle = \langle 1, \chi_W \rangle \langle 1, \chi_{W^c} \rangle.$$

Bevis. Stoppar vi in den reellvärda funktionen φ_W i formel (7) så får vi

$$\langle (I - M)\varphi_W, \varphi_W \rangle = \frac{1}{2N} \sum_{x,y \in V_\Gamma} a(x,y)(\chi_W(x) - \chi_W(y))^2,$$

eftersom konstanterna $\langle 1, \chi_W \rangle$ tar ut varandra. De enda termerna i denna summan som är nollskiljda svarar mot par (x, y) av grannoder, där den ena ligger i W och den andra i W^c. Varje sådant par räknas två gånger i denna summan. Varje sådan term är lika med antalet kanter som binder samman ett sådant par av noder. Alltså är summan lika med $2|\mathcal{E}(W)|$, och vi får

$$\langle (I - M)\varphi_W, \varphi_W \rangle = \frac{2|\mathcal{E}(W)|}{2N} = \frac{|\mathcal{E}(W)|}{N}.$$

Vi beräknar nu $\langle \varphi_W, \varphi_W \rangle$. Notera att funktionerna $\varphi_W = \chi_W - \langle 1, \chi_W \rangle$ är ortogonala mot delrummet av $L^2(\Gamma)$ bestående av konstanta funktioner. För vi har $\langle 1, \varphi_W \rangle = \langle 1, \chi_W \rangle - \overline{\langle 1, \chi_W \rangle} = 0$, eftersom $\langle 1, \chi_W \rangle = \frac{1}{N} \sum_{x \in V_\Gamma} \overline{\chi_W(x)} \deg(x)$ är reellt. Så vi har

$$\langle \varphi_W, \chi_W - \langle 1, \chi_W \rangle \rangle = \langle \chi_W, \chi_W \rangle - \langle 1, \chi_W \rangle^2.$$

Eftersom $\langle \chi_W, \chi_W \rangle = \langle 1, \chi_W \rangle = \frac{1}{N} \sum_{x \in W} \deg(x) =: \mu_W$ så får vi

$$\langle \varphi_W, \varphi_W \rangle = \mu_W(1 - \mu_W) = \mu_W \mu_{W^c} = \langle 1, \chi_W \rangle \langle 1, \chi_{W^c} \rangle,$$

där vi har använt att

$$\begin{aligned} 1 - \mu_W &= \frac{1}{N}\big(N - \sum_{x \in W} \deg(x)\big) \\ &= \frac{1}{N} \sum_{x \in W^c} \deg(x) = \mu_{W^c} = \langle 1, \chi_{W^c} \rangle. \end{aligned}$$

□

Lemma 3.8. *Om $W \subseteq V_\Gamma$ så gäller*

$$N \langle 1, \chi_W \rangle \langle 1, \chi_{W^c} \rangle \geq \frac{(v_-)^2}{v_+} \frac{|W||W^c|}{|V_\Gamma|}.$$

Bevis. Vi har

$$N \langle 1, \chi_W \rangle = \sum_{x \in V_\Gamma} \chi_W(x) \deg(x) = \sum_{x \in W} \deg(x) \geq |W| v_-.$$

Vi har också

$$\langle 1, \chi_{W^c} \rangle = \frac{\sum_{x \in W^c} \deg(x)}{\sum_{x \in V_\Gamma} \deg(x)} \geq \frac{|W^c| v_-}{|V| v_+}.$$

Multiplicerar vi dessa två olikheterna så får vi påståendet. □

Vi kan nu bevisa Sats 3.3.

Bevis av Sats 3.3. Vi har

$$\lambda_1(\Gamma) = \min_{0\neq\varphi\perp 1} \frac{\langle (I-M)\varphi,\varphi\rangle}{\langle\varphi,\varphi\rangle} \leq \min_{\varnothing\neq W\subseteq V_\Gamma,\ |W|\leq |V_\Gamma|/2} \frac{\langle (I-M)\varphi_W,\varphi_W\rangle}{\langle\varphi_W,\varphi_W\rangle}$$

eftersom φ_W är ortogonal mot dom konstanta funktionerna. Lemma 3.7 ger oss då

$$\lambda_1(\Gamma) \leq \min_{\varnothing\neq W\subseteq V_\Gamma,\ |W|\leq |V_\Gamma|/2} |\mathcal{E}(W)| \frac{1}{N\langle 1,\chi_W\rangle\langle 1,\chi_{W^c}\rangle}.$$

Använder vi nu Lemma 3.8 så får vi

$$\lambda_1(\Gamma) \leq \min_{\varnothing\neq W\subseteq V_\Gamma,\ |W|\leq |V_\Gamma|/2} |\mathcal{E}(W)| \frac{v_+}{(v_-)^2} \frac{|V_\Gamma|}{|W||W^c|}.$$

Eftersom vi antar att $|W| \leq |V_\Gamma|/2$ så gäller

$$\frac{|V_\Gamma|}{|W^c|} = \frac{1}{1-\frac{|W|}{|V_\Gamma|}} \leq \frac{1}{1-\frac{1}{2}} = 2.$$

Alltså får vi

$$\lambda_1(\Gamma) \leq \min_{\varnothing\neq W\subseteq V_\Gamma,\ |W|\leq |V_\Gamma|/2} \frac{|\mathcal{E}(W)|}{|W|} \frac{2v_+}{(v_-)^2} = \frac{2v_+}{(v_-)^2} h(\Gamma).$$

□

4 Margulis konstruktion

De hårda kraven för att en familj av grafer ska vara en expanderfamilj gör det inte uppenbart att sådana grafer skulle kunna finnas. I Appendix E ges ett probabilistiskt bevis av existensen av expandergrafer. Detta bevis säger dock ingenting om hur man explicit konstruerar sådana grafer, något som är intressant i praktiska sammanhang. I detta avsnitt ska vi ge ett konkret exempel på en expandergraf, nämligen Margulis konstruktion, och visa att den uppfyller kraven för expandergrafer. I beviset undersöker vi en familj av grafer vars noder är elementen i en abelsk grupp. Graferna kommer vi se är sammanhängande och definieras dessutom på ett sådant sätt att de blir reguljära. För att visa att graferna är en expanderfamilj räcker det då, enligt Sats 3.3, att visa att det minsta nollskilda egenvärdet λ_1 till $I-M$ för alla grafer i familjen är större än eller lika med något positivt k. Detta gör vi genom att använda fouriertransform och istället visa en olikhet för $\langle\widehat{Mf},\hat{f}\rangle$. Denna kommer vi kunna bevisa genom att göra konkreta beräkningar.

Utgångspunkten för konstruktionen är de fyra matriserna:

$$T_1 = \begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}, T_2 = \begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}, e_1 = \begin{bmatrix}1\\ 0\end{bmatrix}, e_2 = \begin{bmatrix}0\\ 1\end{bmatrix}.$$

Med hjälp av dessa kan vi definiera de fyra linjära avbildningarna

$$A_1(\mu) = T_1\mu,\ A_2(\mu) = T_2\mu,\ A_1^{-1}(\mu) = T_1^{-1}\mu,\ A_2^{-1}(\mu) = T_2^{-1}\mu,$$

och de fyra affina avbildningarna

$$B_1(\mu) = T_1\mu + e_1,\ B_2(\mu) = T_2\mu + e_2,\ B_1^{-1}(\mu) = T_1^{-1}\mu - T_1^{-1}e_1,\ B_2^{-1}(\mu) = T_2^{-1}\mu - T_2^{-1}e_2.$$

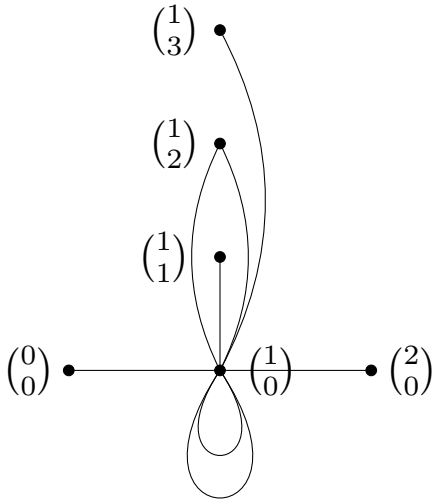
Vi låter nu S vara en symmetrisk mängd som innehåller dessa avbildningar, nämligen

$$S = \{A_1^{\pm 1}, A_2^{\pm 1}, B_1^{\pm 1}, B_2^{\pm 1}\}$$

Familjen av grafer vi ska undersöka är $\Gamma_n = (V_n, E_n, \mathrm{ep})$ där V_n är den abelska gruppen $(\mathbb{Z}/n\mathbb{Z})^2$, och kantmängden ges av

$$E_n = \{(s, \mu) \mid s \in S,\ \mu \in V_n\}/\sim,$$

där $(s, \mu) \sim (s', \mu')$ om och endast om $\mu' = s\mu$ och $s' = s^{-1}$. Ändpunktsavbildningen definieras sedan som $(s, \mu) \mapsto \{\mu, s\mu\}$. De åtta grannarna till en nod μ, där en granne kan förekomma flera gånger, ges alltså av alla $s\mu$ där $s \in S$. Figur 1 illustrerar hur noden $(1, 0)^{\mathrm{T}}$ kopplas till dess grannar i fallet då $n = 4$. Notera speciellt att vi endast är intresserade av resten vid division med 4 av resultatet som fås genom att stoppa in vektorn i de affina- och linjära avbildningarna.



Figur 1: Grafen Γ_n i fallet då n = 4. Denna visar endast hur $(1, 0)^T$ kopplas till dess grannar.

För en nod $\mu = (x, y)^T$ gäller det att $B_1(A_1^{-1}(\mu)) = \mu + e_1$ och att $B_2(A_2^{-1}(\mu)) = \mu + e_2$ vilket betyder att grafen är sammanhängande. Eftersom graferna Γ_n dessutom är 8-reguljära så säger Sats 3.3 att om det finns $\lambda > 0$ så att $\lambda_1(\Gamma_n) \geq \lambda$ för alla n i $\mathbb{Z}^+$ så är familjen (Γ_n) en expanderfamilj. Vi bevisar att det finns ett sådant λ genom att visa att det finns ett $\delta < 1$ så att

$$|\langle Mf, f\rangle| \leq \delta \|f\|^2, \quad \forall f \in L^2(\Gamma_n),\ f \perp 1. \tag{8}$$

Detta är för att om (8) gäller så följer det att

$$\langle (I - M)f, f\rangle = \|f\|^2 - \langle Mf, f\rangle \geq (1 - \delta)\|f\|^2, \quad f \perp 1$$

vilket betyder att

$$\lambda_1(\Gamma_n) = \min_{0 \neq f \perp 1} \frac{\langle (I - M)f, f\rangle}{\|f\|^2} \geq (1 - \delta) > 0.$$

Eftersom graferna (Γ_n) är 8-reguljära blir Markovoperatorn, definierad i Ekvation (5), av formen

$$\begin{aligned} Mf(\mu) &= \frac{1}{|S|} \sum_{s \in S} f(s\mu) \\ &= \frac{1}{8}(f(A_1\mu) + f(A_1^{-1}\mu) + f(A_2\mu) + f(A_2^{-1}\mu) \\ &+ f(B_1\mu) + f(B_1^{-1}\mu) + f(B_2\mu) + f(B_2^{-1}\mu)). \end{aligned}$$

Sats 4.1. *Det finns ett $\delta < 1$, oberoende av n, så att för $f \in L^2(\Gamma_n)$ med egenskapen att $f \perp 1$ gäller det att*

$$|\langle Mf, f\rangle| \leq \delta \|f\|^2.$$

För att att bevisa ovanstående sats ska vi istället studera Fouriertransformenerna av Mf och f. Detta är för att villkoret $f \perp 1$ är ekvivalent med $\hat{f}(0) = 0$ som är lättare att hantera. Med hjälp av (C.2) kan vi formulera det ekvivalenta påståendet till Sats 4.1:

$$|\langle \widehat{Mf}, \hat{f} \rangle| \leq \delta \|\hat{f}\|^2, \quad \forall f \in L^2(\Gamma_n) \text{ med } \hat{f}(0) = 0 \tag{9}$$

Från (C.1) ser vi att fouriertransformen för $f \in L^2(\Gamma_n)$ är av formen

$$\hat{f}(\mu) = \frac{1}{n^2} \sum_{x \in V_n} f(x) \overline{\chi_\mu(x)},$$

där

$$\chi_\mu(x) = e^{2\pi i \frac{\mu \cdot x}{n}}.$$

Genom att utveckla den inre produkten i vänsterledet i Ekvation (9) och använda Ekvationerna (27)-(29), får vi att

$$\begin{aligned} &\Big| \frac{1}{8} \sum_{\mu \in V_n \setminus 0} \Big[(1 + \chi_\mu(e_1)) \hat{f}(T_2^{-1}\mu) + (1 + \chi_\mu(e_2)) \hat{f}(T_1^{-1}\mu) \\ &+ (1 + \chi_\mu(-e_1)) \hat{f}(T_2\mu) + (1 + \chi_\mu(-e_2)) \hat{f}(T_1\mu) \Big] \overline{\hat{f}(\mu)} \Big| \\ &\leq \delta \sum_{\mu \in V_n \setminus 0} |\hat{f}(\mu)|^2. \end{aligned} \tag{10}$$

Notera att vi exkluderat 0 ur de μ vi summerar över. Detta kommer från att $\hat{f}(0) = 0$, och observationen att termen då $\mu = 0$ i summan därför blir noll. Användning av triangelolikheten i vänsterledet introducerar faktorer

$$|1 + \chi_\mu(\pm e_j)| = 2|\cos \frac{\pi \mu_j}{n}|,$$

i summans termer. Det motiverar definitionen av en funktion $\gamma : V_n^2 \to \mathbb{R}$ med följande egenskaper: för alla $\mu, \nu \in V_n \setminus \{(0,0)\}$ gäller att

$$\gamma(\mu, \nu)\gamma(\nu, \mu) = 1, \tag{11}$$

och

$$|\cos \frac{\pi \mu_1}{n}|(\gamma(\mu, T_2\mu) + \gamma(\mu, T_2^{-1}\mu)) + |\cos \frac{\pi \mu_2}{n}|(\gamma(\mu, T_1\mu) + \gamma(\mu, T_1^{-1}\mu)) \leq 4\delta. \tag{12}$$

För att se varför defintionen av γ är motiverad, låt först $G(\mu) = |\hat{f}|$. Tringelolikheten, och olikheten $2ab \leq \gamma a^2 + \frac{1}{\gamma} b^2$, under antagandet att $\gamma > 0$, ger då att vänsterledet (VL) i Ekvation (10) är

$$\begin{aligned} VL &\leq \frac{1}{8} \sum_{\mu \in V_n \setminus 0} \Big[|1 + \chi_\mu(e_1)| G(T_2^{-1}\mu) G(\mu) + |1 + \chi_\mu(e_2)| G(T_1^{-1}\mu) G(\mu) \\ &+ |1 + \chi_\mu(-e_1)| G(T_2\mu) G(\mu) + |1 + \chi_\mu(-e_2)| G(T_1\mu) G(\mu) \Big] \\ &\leq \frac{1}{8} \sum_{\mu \in V_n \setminus 0} \Big[|\cos \frac{\pi \mu_1}{n}|(\gamma(\mu, T_2^{-1}\mu) + \gamma(T_2^{-1}\mu, \mu)) + |\cos \frac{\pi \mu_2}{n}|(\gamma(\mu, T_1^{-1}\mu) + \gamma(T_1^{-1}\mu, \mu)) \\ &+ |\cos \frac{\pi \mu_1}{n}|(\gamma(\mu, T_2\mu) + \gamma(T_2\mu, \mu)) + |\cos \frac{\pi \mu_2}{n}|(\gamma(\mu, T_1\mu) + \gamma(T_1\mu, \mu)) \Big] G^2(\mu) \\ &\leq \frac{1}{4} \sum_{\mu \in V_n \setminus 0} \Big[|\cos \frac{\pi \mu_1}{n}|(\gamma(\mu, T_2^{-1}\mu) + \gamma(\mu, T_2\mu)) \\ &+ |\cos \frac{\pi \mu_2}{n}|(\gamma(\mu, T_1^{-1}\mu) + \gamma(\mu, T_1\mu)) \Big] G^2(\mu) \\ &\leq \delta \sum_{\mu \in V_n \setminus 0} |\hat{f}(\mu)|^2, \end{aligned}$$

där vi i den andra olikheten har använt Ekvation (11), i den tredje olikheten substitutionen $\mu' = T_j^{\pm 1}\mu$ (notera att $T_j^{\pm}V_n = V_n$, och att μ-komponenten i cosinusfaktorn inte påverkas av respektive substitution), och i den sista olikheten Ekvation (12). Detta betyder att om vi kan finna en positiv funktion γ med egenskaperna i Ekvation (11) och (12) så är Sats 4.1 bevisad.

För att definiera γ inför vi först en partiell ordning $<$ på V_n. För alla $\mu = (\mu_1, \mu_2) \in V_n$, låt

$$a(\mu_j) = \begin{cases} \mu_j & 0 \leq \mu_j \leq \frac{n}{2} \\ n - \mu_j & \frac{n}{2} \leq \mu_j \leq n \end{cases}.$$

Vi säger då att $\mu < \mu'$ om $a(\mu_1) \leq a(\mu_1')$ och $a(\mu_2) \leq a(\mu_2')$, och en av olikheterna är strikt. I annat fall säger vi att μ och μ' är ojämförbara. Definitionen av γ tas då till att vara

$$\gamma(\mu, \mu') = \begin{cases} \alpha & \mu' < \mu \\ \frac{1}{\alpha} & \mu < \mu' \\ 1 & \mu, \mu' \text{ ojämförbara} \end{cases},$$

där $\alpha = 5/4$. Denna definition av γ satisfierar uppenbarligen Ekvation (11). För att se att den också satisfierar Ekvation (12), låt oss betrakta två fall: (i) $a(\mu_1) + a(\mu_2) \geq \frac{n}{2}$, (ii) $a(\mu_1) + a(\mu_2) < \frac{n}{2}$.

I fall (i) kan vänsterledet i Ekvation (12) överskattas genom att ta alla γ till att vara α. Vi vill då visa att

$$|\cos(\frac{\pi\mu_1}{n})| + |\cos(\frac{\pi\mu_2}{n})| \leq \frac{8\delta}{5}, \tag{13}$$

för något $\delta < 1$. Av symmetri är det tillräckligt att betrakta fallet då $0 \leq \mu_1, \mu_2 \leq n/2$. Då är $|\cos\frac{\pi\mu_j}{n}| = \cos\frac{\pi\mu_j}{n}$ och $a(\mu_j) = \mu_j$. Notera att $\cos\frac{\pi\mu_2}{n}$ är minskande för ett givet μ_1, varför maximum av vänsterledet i Ekvation (13) antas vid $\mu_2 = n/2 - \mu_1$. Vi får alltså uppskattningen

$$\cos\frac{\pi\mu_1}{n} + \cos\frac{\pi\mu_2}{n} \leq \cos\frac{\pi\mu_1}{n} + \cos\left(\frac{\pi}{2} - \frac{\pi\mu_1}{n}\right) = \sqrt{2}\sin\left(\frac{\pi}{4} + \frac{\pi\mu_1}{n}\right) \leq \sqrt{2}.$$

vilket visar att γ satisfierar Ekvation (12) i fall (i) för $0.84 < \delta < 1$.

I fall (ii) överskattar vi vänsterledet i Ekvation (12) genom att ta cosinusfaktorerna till att vara 1. Vi vill då visa att

$$\gamma(\mu, T_2\mu) + \gamma(\mu, T_2^{-1}\mu) + \gamma(\mu, T_1\mu) + \gamma(\mu, T_1^{-1}\mu) \leq 4\delta, \tag{14}$$

för något $\delta < 1$. Antag först att $a(\mu_1) = a(\mu_2)$. Då har vi antingen $\mu_1 = \mu_2$ eller $\mu_1 = n - \mu_2$. Om $\mu_1 = \mu_2$ fås

$$\begin{cases} a(\mu_1 - 2\mu_2) = a(-\mu_1) = a(\mu_1) \\ a(\mu_2 - 2\mu_1) = a(-\mu_2) = a(\mu_2) \\ a(\mu_1 + 2\mu_2) = a(3\mu_1) > a(\mu_1) \\ a(\mu_2 + 2\mu_1) = a(3\mu_2) > a(\mu_2) \end{cases}$$

där vi i de två olikheterna har använt att

$$\mu_i < n/4 \implies 3\mu_i < 3n/4 \implies n/4 \leq 3\mu_i < 3n/4,$$

alltså att $3\mu_i$ ligger närmare $n/2$ än μ_i. Detta visar att $\gamma(\mu, T_1^{-1}\mu) = \gamma(\mu, T_2^{-1}\mu) = 1$, och $\gamma(\mu, T_1\mu) = \gamma(\mu, T_2\mu) = 1/\alpha$, vilket satisfierar Ekvation (14) för $0.9 < \delta < 1$. Samma resultat fås då $\mu_1 = n - \mu_2$.

Antag nu att $a(\mu_1) > a(\mu_2)$. Vi har då följande fyra fall att skilja mellan.

$$\begin{cases} n/2 > \mu_1 > \mu_2 \geq 0 \\ n/2 < \mu_1 < \mu_2 \leq n \\ n/2 > \mu_1 > 0 \ \text{ och } \ n/2 < \mu_2 \leq n \\ n/2 < \mu_1 < n \ \text{ och } \ n/2 > \mu_2 \geq 0 \end{cases}$$

Om till exempel $n/2 > \mu_1 > 0$ och $n/2 < \mu_2 \leq n$, kan vi skriva $n/2 > \tilde{\mu_1} > \tilde{\mu_2} \geq 0$, där $\tilde{\mu_1} = \mu_1$, och $\tilde{\mu_2} = n - \mu_2$. Men eftersom

$$\begin{cases} a(\mu_1 - 2\mu_2) = a(\tilde{\mu_1} - 2n + 2\tilde{\mu_2}) = a(\tilde{\mu_1} + 2\tilde{\mu_2}) \\ a(\mu_2 - 2\mu_1) = a(n - \tilde{\mu_2} - 2\tilde{\mu_1}) = a(\tilde{\mu_2} + 2\tilde{\mu_1}) \\ a(\mu_1 + 2\mu_2) = a(\tilde{\mu_1} + 2n - 2\tilde{\mu_2}) = a(\tilde{\mu_1} - 2\tilde{\mu_2}) \\ a(\mu_2 + 2\mu_1) = a(n - \tilde{\mu_2} + 2\tilde{\mu_1}) = a(\tilde{\mu_2} - 2\tilde{\mu_1}) \end{cases}$$

ser vi att detta resultat följer av resultatet då $n/2 > \mu_1 > \mu_2 \geq 0$. Motsvarande kan visas för de andra fallen, varför det är tillräckligt att betrakta fallet då $n/2 > \mu_1 > \mu_2 \geq 0$. Vi får då att

$$\begin{cases} \mu_1 - \mu_2 > 0 \implies \mu_1 - 2\mu_2 > -\mu_2 > -\mu_1 \implies -\mu_1 < \mu_1 - 2\mu_2 < \mu_1 \implies \gamma(\mu, T_1^{-1}\mu) = \alpha \\ \mu_2 < n/2 - \mu_1 \implies \mu_1 + 2\mu_2 < n - \mu_1 \implies \mu_1 < \mu_1 + 2\mu_2 < n - \mu_1 \implies \gamma(\mu, T_1\mu) = \frac{1}{\alpha} \\ \mu_1 < n/2 - \mu_2 \implies \mu_2 + 2\mu_1 < n - \mu_2 \implies \mu_2 < \mu_2 + 2\mu_1 < n - \mu_2 \implies \gamma(\mu, T_2\mu) = \frac{1}{\alpha} \\ \mu_2 - \mu_1 < 0 \implies \mu_2 - 2\mu_1 < -\mu_1 < -\mu_2 \implies \mu_2 - n < \mu_2 - 2\mu_1 < -\mu_2 \implies \gamma(\mu, T_2^{-1}\mu) = \frac{1}{\alpha} \end{cases}$$

Alltså gäller Ekvation (14) för $0.92 < \delta < 1$. Samma resultat fås då $a(\mu_2) > a(\mu_1)$, vilket ses med omnumreringen $1 \longleftrightarrow 2$. Alltså finns ett $\delta < 1$ så att γ satisfierar Ekvation (11) och Ekvation (12), och Sats 4.1 är därmed bevisad.

5 Gowers sats

Vi börjar detta kapitel med att studera den cykliska gruppen $G = \mathbb{Z}/2k\mathbb{Z}$ där $k \geq 1$ är ett heltal. Vi låter A och B vara delmängderna

$$A = \{g \in G \mid g \text{ udda}\} \quad \text{och} \quad B = \{g \in G \mid g \text{ jämn}\}.$$

Om $a_1, a_2 \in A$ så gäller det att $a_1 + a_2 \in B$. Detta tillsammans med observationen att $A + \{1\} = B$ ger oss att $A + A = B$. Genom ett liknande resonemang inser man att $B + A = A$. Vi får då att

$$mA = \underbrace{A + A + \cdots + A}_{m \text{ stycken}} = \begin{cases} A, & m \text{ udda} \\ B, & m \text{ jämn} \end{cases}$$

Detta betyder att mA aldrig kan bli hela G oavsett värdet av m trots att A innehåller hälften av alla element i G. Vi kommer härnäst visa att detta inte är något som gäller för gruppen $SL(2, \mathbb{F}_p)$. Nämligen, om A är en tillräckligt stor delmängd så kommer dess trippelprodukt att bli hela $SL(2, \mathbb{F}_p)$.

Sats 5.1 (Gowers)**.** *Låt p vara ett primtal. Om $A \subset SL(2, \mathbb{F}_p)$ är en symmetrisk delmängd, och $|A| \geq 2|SL(2, \mathbb{F}_p)|^{8/9}$, då är $A^3 = SL(2, \mathbb{F}_p)$.*

I beviset använder vi att egenvärdena $\lambda \neq 1$ till Markovoperatorn $M : L^2(G) \to L^2(G)$, som definieras enligt

$$Mf(x) = \frac{1}{|A|} \sum_{s \in A} f(xs), \tag{15}$$

är till beloppet mycket mindre än 1, då $G = SL(2, \mathbb{F}_p)$. Gruppen G tillsammans med dess symmetriska delmängd A bildar *Cayleygrafen* $\Gamma(G, A)$ till G. Detta är en oriktad A-reguljär graf utan multipla kanter med gruppelementen i G som noder. Två noder $g, h \in G$ har en kant mellan sig

om och endast om det finns $a \in A$ så att $ga = h$. Detta gör att vi kan tolka funktioner på gruppen som funktioner på dess Cayleygraf och att Markovoperatorn i (15) motsvarar Markovoperatorn i (5).

En följd av Gowers sats är att diametern, definierad i (3), av motsvarande Cayleygraf $\Gamma(G, A)$ är som mest 3. Detta är för att om $g, h \in SL(2, \mathbb{F}_p)$ så finns det $a_1, a_2, a_3 \in A$ så att $a_1a_2a_3 = g^{-1}h$ och därmed $g(a_1a_2a_3) = h$. Detta är intressant för att trots att A är väldigt liten i förhållande till G asymptotiskt så är noderna i $\Gamma(G, A)$ inte mer än 3 kanter ifrån varandra.

Innan vi kan bevisa Gowers sats så behöver vi först några hjälpsatser. Speciellt viktig är Frobenius sats som presenteras och bevisas nedan.

Sats 5.2 (Frobenius)**.** *Låt $G = SL(2, \mathbb{F}_p)$ där p är ett primtal och $\varphi : G \to GL(V)$ vara en icke-trivial unitär representation av G. Då är $d_\varphi = dim(V) \geq \frac{p-1}{2}$.*

Bevis. Om $p = 2$ är det uppenbart att olikheten gäller eftersom varje representation är åtminstone av grad 1. Vi antar därför i fortsättningen att $p \geq 3$. Från (D.2) vet vi att

$$T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{och} \quad T_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

genererar gruppen G. Eftersom φ är icke-trivial betyder det att $\varphi(T_1) \neq I$ eller $\varphi(T_2) \neq I$. Detta är för att varje element $g \in G$ kan skrivas som en produkt av T_1 och T_2, så om både $\varphi(T_1) = I$ och $\varphi(T_2) = I$ skulle det då följa att $\varphi(g) = I$, eftersom φ är en homomorfi. Vi kan anta utan inskränkning att $\varphi(T_1) \neq I$. Eftersom $\varphi(T_1)$ är unitär, och därmed normal, så följer det från (A.9) att $\varphi(T_1)$ är diagonaliserbar. Detta innebär att det måste finnas ett egenvärde λ till $\varphi(T_1)$ som är skiljt från ett, för annars hade det funnits en bas $(e_1, \ldots, e_n)$ av V så att $\varphi(T_1)e_i = e_i$ för alla $i = 1, \ldots, n$, vilket endast är möjligt om $\varphi(T_1) = I$.

Om $\mu \in \mathbb{F}_p^*$ så har vi

$$\begin{bmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \mu^{-1} & 0 \\ 0 & \mu \end{bmatrix} = \begin{bmatrix} 1 & \mu^2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\mu^2}$$

där $\mu^2 \in \mathbb{F}_p^*$. Notera att detta är väldefinierat, för om $m = \mu^2 + kp$ så har vi

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^m = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\mu^2+kp} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\mu^2}$$

eftersom

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^p = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Detta medför att

$$A^{\mu^2} = \varphi\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\mu^2}\right) = \underbrace{\varphi\left(\begin{bmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{bmatrix}\right)}_{=:T} \underbrace{\varphi\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)}_{=:A} \underbrace{\varphi\left(\begin{bmatrix} \mu^{-1} & 0 \\ 0 & \mu \end{bmatrix}\right)}_{T^{-1}} = TAT^{-1} \tag{16}$$

Vi gör nu den enkla observationen att A^{μ^2} har egenvärdet λ^{μ^2} eftersom λ är ett egenvärde till A. Från (16) följer det att varje egenvärde till A^{μ^2} också är ett egenvärde till A. För antag att τ är ett egenvärde till A^{μ^2}, och att u är en egenvektor som hör till τ. Då har vi $A(T^{-1}u) = T^{-1}A^{\mu^2}TT^{-1}u = T^{-1}A^{\mu^2}u = \tau(T^{-1}u)$. Alltså är då τ även ett egenvärde till A. Eftersom $\lambda \neq 1$ innebär detta att A har minst lika många olika egenvärden som det finns olika kvadrater i $\mathbb{F}_p^*$. För att bestämma antalet sådana kvadrater studerar vi följande homomorfi

$$\phi : \mathbb{F}_p^* \to \mathbb{F}_p^*, \; x \mapsto x^2.$$

Att ϕ är en homomorfi följer av att för $g, h \in \mathbb{F}_p^*$ så gäller

$$\phi(gh) = (gh)^2 = ghgh = gghh = \phi(g)\phi(h)$$

där vi använt att $\mathbb{F}_p^*$ är abelsk. Eftersom $\mathbb{F}_p^*/\ker(\phi)$ är isomorf med $\phi(\mathbb{F}_p^*)$ får vi att $|\phi(\mathbb{F}_p^*)| = |\mathbb{F}_p^*|/|\ker(\phi)|$. Notera att $\ker(\phi) = \{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{1, -1\}$. Alltså är antalet kvadrater i $\mathbb{F}_p^*$ lika med $(p-1)/2$. Eftersom egenvektorer till olika egenvärden är linjärt obereoende följer det att

$$d_\varphi = \dim(V) \geq \frac{p-1}{2}.$$

□

Lemma 5.3. *Låt $G = SL(2, \mathbb{F}_p)$, och låt $A \subset G$ vara en symmetrisk delmängd. Egenvärdena $\lambda \neq 1$ till Markovoperatorn uppfyller olikheten*

$$|\lambda| \leq \sqrt{\frac{2|G|}{(p-1)|A|}}.$$

Bevis. Vi börjar med att beräkna spåret av M^2. Vi har

$$M^2 f(x) = \frac{1}{|A|} \sum_{s \in A} Mf(xs) = \frac{1}{|A|^2} \sum_{s \in A} \sum_{t \in A} f(xst).$$

Spåret av M^2 ges då av

$$\sum_{x \in G} M^2 \delta_x(x) = \frac{1}{|A|^2} \sum_{x \in G} \sum_{s,t \in A} \delta_x(xst) = \frac{1}{|A|^2} |G||A|.$$

Å andra sidan vet vi att spåret av M ges av summan av dess egenvärden, då M är en självadjungerad operator. Det följer att spåret av M^2 ges av summan av kvadraterna av egenvärdena till M. Så vi har

$$\frac{|G|}{|A|} = \sum_i \lambda_i^2,$$

där λ_i är egenvärdena till M. Notera att antalet gånger en term λ_i^2 förekommer i summan ovan är minst lika stor som den geometriska multipliciteten av λ_i.

Vi ser enkelt att $M\pi_g = \pi_g M$, där π är den reguljära representationen. Om λ är ett egenvärde till M, och v är en egenvektor hörande till λ så gäller $M\pi_g v = \pi_g M v = \pi_g \lambda v = \lambda \pi_g v$. Alltså är egenrummet hörande till λ ett G-invariant delrum, så om vi begränsar π till detta egenrum får vi en representation av G som inte är trivial om $\lambda \neq 1$. Av Lemma B.3 och Sats 5.2 följer då att detta egenrum har dimension större än eller lika med $(p-1)/2$. Av detta får vi följande uppskattning:

$$\frac{|G|}{|A|} \geq \frac{p-1}{2} \lambda_j^2$$

för varje $\lambda_j \neq 1$. □

Nedan betecknar χ den karaktäristiska funktionen given i Definition 3.6.

Lemma 5.4. *Låt $A \subset G$. Om $\langle M\chi_A, \chi_{gA^{-1}} \rangle \neq 0$, för alla $g \in G$, så är $A^3 = G$.*

Bevis. Antag att $A^3 \neq G$. Då finns ett $g \in G$ sådant att $g \notin A^3$. Olikheten

$$0 \neq \langle M\chi_A, \chi_{gA^{-1}} \rangle = \frac{1}{|G||A|} \sum_{x \in G} \sum_{a \in A} \chi_A(xa) \chi_{gA^{-1}}(x)$$

kan gälla endast om det finns ett $x \in G$ sådant att $xa \in A$ och $x \in gA^{-1}$. Men det implicerar att $x \in A^2$ och $g \in xA$, och alltså $g \in A^3$, vilket är en motsägelse. □

Vi är nu redo att bevisa Gowers sats.

Bevis av Sats 5.1. Låt e_i, med $i \in \{0, \dots, |G|-1\}$, beteckna baselementen i en ON-bas för $L^2(G)$ bestående av egenvektorer till M, och låt g vara ett element i G. Med den omvända triangelolikheten blir

$$|\langle M\chi_A, \chi_{gA^{-1}}\rangle| \geq |\lambda_0\langle\chi_A, e_0\rangle\langle e_0, \chi_{gA^{-1}}\rangle| - |\sum_{i\geq 1}\lambda_i\langle\chi_A, e_i\rangle\langle e_i, \chi_{gA^{-1}}\rangle|, \tag{17}$$

efter att ha utvecklat χ_A i egenbasen. Låt oss beteckna egenvärdet 1, som hör till de konstanta funktionerna, med λ_0. Den motsvarande vektorn i egenbasen, e_0, kan väljas till funktionen som är lika med 1 på alla noder. Genom att skriva ut summan för respektive skalärprodukt syns att

$$|\lambda_0\langle\chi_A, e_0\rangle\langle e_0, \chi_{gA^{-1}}\rangle| = \frac{|A|^2}{|G|^2}. \tag{18}$$

Vidare kan den andra termen i högerledet av Ekvation (17) uppskattas med Cauchy-Schwarz olikhet enligt

$$|\sum_{i\geq 1}\lambda_i\langle\chi_A, e_i\rangle\langle e_i, \chi_{gA^{-1}}\rangle| \leq \max_{i\geq 1}|\lambda_i|\sqrt{\sum_{i\geq 1}|\langle\chi_A, e_i\rangle|^2}\sqrt{\sum_{i\geq 1}|\langle e_i, \chi_{gA^{-1}}\rangle|^2}. \tag{19}$$

Notera att

$$\sum_{i\geq 1}|\langle\chi_A, e_i\rangle|^2 \leq \sum_{i\geq 0}|\langle\chi_A, e_i\rangle|^2 = ||\chi_A||^2 = \frac{|A|}{|G|},$$

där den näst sista likheten följer av att egenbasen är ortonormal. På samma vis kan den andra summan i högerledet av Ekvation (19) uppskattas med $|A|/|G|$. Tillsammans med Lemma 5.3 blir alltså

$$|\sum_{i\geq 1}\lambda_i\langle\chi_A, e_i\rangle\langle e_i, \chi_{gA^{-1}}\rangle| \leq \sqrt{\frac{2|A|}{(p-1)|G|}}. \tag{20}$$

Sammantaget får vi med insättning av Ekvation (18) och (20) i Ekvation (17) att

$$|\langle M\chi_A, \chi_{gA^{-1}}\rangle| \geq \frac{|A|^2}{|G|^2} - \sqrt{\frac{2|A|}{(p-1)|G|}}. \tag{21}$$

Högerledet i Ekvation 21 är strikt större än noll om

$$|A| > \frac{2^{1/3}|G|^{1/9}}{(p-1)^{1/3}}|G|^{8/9},$$

och med $|G|$ given av Proposition D.1 gäller för alla $p \geq 2$ att

$$1 < \frac{2^{1/3}|G|^{1/9}}{(p-1)^{1/3}} < 2. \tag{22}$$

Enligt satsens hypotes är $|A| \geq 2|G|^{8/9}$, och resultatet följer därmed av Lemma 5.4.

□

6 Felrättande koder

I detta kapitel kommer vi att skicka meddelanden som består av symboler från ett visst alfabet. Vid överföring av detta meddelande kan symboler förändras, bli oläsliga, tillkomma eller falla bort enligt olika mönster. Här kommer vi att begränsa till oss till fallet då symboler *singlas*, alltså byter värde inom alfabetet. Oavsett hur ett meddelande ändras vid överföring kommer detta meddelande kunna tolkas som ett legitimt meddelande. Det finns alltså ingen möjlighet att veta att någon ändring har skett. Därför kommer vi att avbilda samtliga meddelanden på längre meddelanden med hjälp av *redundant* information. Dessa längre ord kallas *kodord* och är mer utspridda. Om kodord skickas istället kommer dessa alltså behöva ett större antal förändringar för att denna förväxling kommer att ske. Eftersom ett stort antal fel är osannolikt kommer troligtvis det mottagna kodordet var mest likt det ursprungliga kodordet. Med hjälp av expandergrafer kan vi sedan skapa koder som gör detta.

6.1 Grundläggande informationsteori

För att kunna tala om hur koder fungerar och hur bra dessa koder presterar behöver vi först definiera dessa begrepp och relevanta mått.

Definition 6.1 (Alfabet)**.** Ett alfabet Σ är en ändlig mängd av symboler. Antalet symboler $|\Sigma|$ i ett alfabet betecknas q. Vi låter även Σ^n beteckna rummet av n-tupler med element tagna från Σ.

Dessa tupler beskriver alla de ord som symbolerna i alfabetet bygger upp.

Definition 6.2 (Kod)**.** En kod C från ett alfabet Σ är en delmängd av Σ^n. Elementen i C kallas för kodord.

Det är alltså kodorden som de olika meddelanden kommer att avbildas på. Om dessa avbildningar ligger *långt* ifrån varandra kommer det som sagt kräva ett stort antal fel för att tvetydighet ska kunna uppstå.

Definition 6.3 (Hammingavstånd)**.** Hammingavståndet, d_H, mellan $x, y \in \Sigma^n$ definieras

$$d_H(x, y) = |\{i \mid x_i \neq y_i\}|.$$

Denna definition beskriver alltså antalet koordinater där två tupler skiljer sig åt och kan visas vara en metrik på Σ^n. Antalet fel kan nu definieras som ett avstånd i den här metriken. Detta kommer visa sig vara viktigt för hur felrobust en kod kan vara.

Definition 6.4 (Avstånd)**.** Avståndet, d, för en kod, $C \subseteq \Sigma^n$ definieras som

$$d(C) = \min_{c_1 \neq c_2} d_H(c_1, c_2)$$

där $c_1, c_2 \in C$.

Varje par av kodord kommer alltså att ha ett utrymme mellan sig som inte ingår i mängden C. Då vi har begränsat oss till att bara skicka kodord betyder detta att om vi mottar ett ord som inte är ett kodord så måste ett fel ha uppstått och felet upptäcks. Då antalet fel mest troligt är litet kommer vi att anta att det kodord som ligger närmast det mottagna ordet i Hammingavstånd är det ursprungliga kodordet och felet rättas till detta. Det största antalet fel som kan upptäckas eller rättas beskrivs av följande lemma.

Lemma 6.5. *För en kod med avstånd $2t+1$ gäller att $2t$ fel kan upptäckas och att t fel kan rättas.*

Bevis. Vi låter u beteckna det skickade kodordet och v vara det mottagna ordet. Vi antar att antalet fel hos v är $d_H(u, v) \leq 2t$. I så fall kan inte v inte vara ett kodord eftersom avståndet annars hade varit $2t$. Antingen så är det mottagna ordet det rätta kodordet eller så är det inget kodord alls. I så fall upptäcks felet.

I det andra fallet antar vi att antalet fel hos v är $d_H(u, v) \leq t$. För ett annat kodord u' har vi $d_H(u, u') \geq 2t + 1$. Triangelolikheten ger oss

$$d_H(u, u') \leq d_H(u, v) + d_H(v, u').$$

Vidare har vi att

$$d_H(v, u') \geq d_H(u, u') - d_H(u, v) \geq (2t + 1) - t = t + 1$$

vilket innebär att felet rättas till u då detta kodord ligger närmast. □

Definition 6.6 (Hastighet)**.** Hastigheten, r, för en kod, $C \subseteq \Sigma^n$, definieras som

$$r(C) = \frac{\log |C|}{n \log |\Sigma|}.$$

Hastigheten visar alltså proportionen av den kod som är användbar (icke-redundant). Ju mer redundant kod, desto högre sannolikhet att åtgärda fel på bekostnad av att hastigheten minskar.

6.1.1 Begränsningar

Vi kommer nu att härleda en undre och en övre gräns på en kods storlek givet att koden har en viss längd och ett visst avstånd. För att göra detta behöver vi först följande definition.

Definition 6.7 (Hammingsfär)**.** Hammingsfären, H, med radie r kring $x \in \Sigma^n$ är mängden

$$H(x, r) = \{y \in \Sigma^n \mid d_H(x, y) \leq r\}.$$

Vi behöver även storleken på denna mängd, dess *volym*.

Lemma 6.8 (Hammingsfärens volym)**.** *Antalet element i H(x,r) då $x \in \Sigma^n$ fås av*

$$|H(x, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Bevis. Alla element som ligger på avstånd i från x fås genom att singla i olika koordinater hos x. Om någon koordinat hade singlats fler än en gång hade detta element inte längre legat på avstånd i från x. Antalet element på ett givet avstånd fås därför kombinatoriskt genom att placera ut dessa singlingar. Det finns $\binom{n}{i}$ sätt att placera ut singlingarna och $(q-1)^i$ sätt att välja vilka symboler som elementen singlas till. Vi summerar sedan för varje individuellt avstånd. □

Vi börjar nu med att visa den undre gränsen.

Sats 6.9 (Gilbert-Varshamovs gräns)**.** *Det existerar en kod $C \subseteq \Sigma^n$ för alla avstånd $d \leq n$ så att*

$$|C| \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}$$

Bevis. Vi visar detta genom att studera en girig algoritm som med exponentiell komplexitet bygger sådana koder. För denna definierar vi först mängderna $S = \Sigma^n$ och $C = \emptyset$. Vi väljer ett godtyckligt element $x \in S$, lägger detta element i C och tar sedan bort alla element som ligger på ett avstånd mindre än d från x. Detta upprepas tills S är tom. Eftersom $|S| = q^n$ från början och antalet element som tas bort vid varje iteration är övre begränsat av Hammingsfärens volym fås antalet iterationer (och därmed antalet kodord) att vara minst kvoten mellan dessa storheter. □

Den övre gränsen gäller för samtliga koder. Koder för vilka likhet gäller kallas för *perfekta koder*.

Sats 6.10 (Hammings gräns)**.** *Alla koder $C \subseteq \Sigma^n$ med avstånd $d \leq n$ uppfyller*

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}$$

där $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Bevis. Enligt Lemma 6.5 kommer alla element i $H(x, t)$ där x är ett kodord att rättas till detta kodord. Detta betyder att inga par av sådana Hammingsfärer kommer att ha någon överlappning då det i så fall hade rått tvetydighet. Koden kan därför delas upp i ett antal sådana sfärer; en för varje kodord. Det totala antalet element i samtliga sfärer $|C||H(x, t)|$ kommer dock att vara övre begränsat av storleken på Σ^n, alltså q^n och resultatet följer. □

Fallet då likhet gäller mellan avstånd och längd är trivialt för båda gränser.

6.1.2 Linjära koder

Expanderkoder tillhör en viktig underklass av koder som kallas linjära koder. Vi kommer här att införa teori som behövs för att studera dessa koder.

Definition 6.11 (Linjär kod)**.** Låt Σ vara en ändlig kropp och låt C vara ett linjärt underrum till Σ^n. Då sägs C vara en linjär kod.

Varje kodord kan nu uttryckas som en linjärkombination av basvektorer i C.

Definition 6.12 (Generatormatris)**.** Låt C vara en linjär kod av dimension k. Om kolonnerna i en matris $G = \Sigma^{n\times k}$ spänner C sägs denna vara en generatormatris för C.

Vi kan med hjälp av generatormatrisen koda ett meddelande $x \in \Sigma^k$ genom en linjär avbildning till ett kodord $Gx \in C$. Generatormatrisen kan väljas så att det ursprungliga meddelandet återfinns i början av kodordet. Detta kallas för standardform och skrivs

$$G = \begin{pmatrix} I_k \\ P \end{pmatrix}$$

där I_k är identitetsmatrisen av storlek k och P är en $n-k \times k$-matris.

En linjär kod kan även definieras utifrån kärnan till det linjära underrummet för en annan linjär kod.

Definition 6.13 (Dualkod)**.** För en linjär kod $C \subseteq \Sigma^n$, så är dess *dualkod*, $C^\perp$, definierad

$$C^\perp = \{z \in \Sigma^n \mid \langle z \cdot c\rangle = 0,\ \forall c \in C\}$$

där $\langle z \cdot c\rangle = \sum_{i=1}^n z_i c_i$ är den inre produkten över Σ.

Med detta kan vi definiera paritetsmatrisen som vi kommer att använda oss av för att skapa expanderkoder.

Definition 6.14 (Paritetsmatris)**.** Generatormatrisen för $C^\perp$, där $C \subseteq \Sigma^n$ är en linjär kod av dimension k, kallas för paritetsmatris för C och betecknas $H = \Sigma^{(n-k)\times n}$.

Detta betyder alltså att $C = \{c \in \Sigma^n \mid Hc = 0\}$. Vi noterar att varje rad i paritetsmatrisen motsvarar ett bivillkor som koordinaterna hos de tillåtna kodorden måste uppfylla. Varje enskild rad beskriver en summa som för koordinaterna måste vara noll.

Särskilt gäller då att standardformen av G har paritetsmatris

$$H = (-P^\top\ I_{n-k}).$$

Vi kommer även behöva följande lemma.

Lemma 6.15 (Avstånd för linjära koder)**.** *Låt $C \subseteq \Sigma^n$ vara en linjär kod. Avståndet för C ges då av*

$$d(C) = w(C) = \min_{\substack{x\in C\\ x\neq 0}} w(x)$$

där $w(x) = d_H(x, 0)$ betecknar vikten av ett kodord x, alltså antalet nollskilda koordinater i x.

Bevis. Vi väljer x, $y \in C$ så att $d(C) = d_H(x, y)$. Enligt antagandet i lemmat gäller då att

$$d(C) = d_H(x, y) = d_H(x - y, 0) = w(x - y) \geq w(C).$$

Omvänt gäller för något $x \in C$ även att

$$w(C) = w(x) = d_H(x, 0) \geq d(C).$$

Alltså, ekvationerna ovan är därmed ekvivalenta med att $d(C) = w(C)$. □

6.2 Expanderkoder

En linjär kod kan alltså definieras utifrån dess generatormatris eller dess paritetsmatris. Strukturen på paritetsmatrisen kan illustreras med så kallade *bipartita* grafer. Med hjälp av expansionkrav och grafteoretiska resonemang kommer koden från denna graf sedan att studeras. Hädanefter är alfabetet $\Sigma = \{0, 1\}$.

Definition 6.16 (Bipartit graf)**.** En graf $\Gamma = (V, E, \mathrm{ep})$ är bipartit om dess nodmängd V kan delas upp i två disjunkta samt icke-tomma delmängder V_0 respektive V_1 så att varje kant har en extremitet i V_0 och en i V_1, så att

$$\mathrm{ep}(\alpha) \cap V_0, \quad \mathrm{ep}(\alpha) \cap V_1 \neq \emptyset, \quad \alpha \in E$$

För denna typ av graf räcker det att partitionera de två delgraferna vilket ger upphov till följande variant av Cheegerkonstanten.

Definition 6.17 (Bipartit expansion)**.** För en ändlig graf $\Gamma = (V, E, \mathrm{ep})$ med en uppdelning $V = V_0 \cup V_1$ skrivs den bipartita expansionen

$$\check{h}(\Gamma) = \min(h_0, h_1)$$

där

$$h_i = \min\left\{ \frac{|\partial W|}{|W|} \mid W \subset V_i, 1 \leq |W| \leq \frac{|V_i|}{2} \right\}.$$

Även denna definition kan användas för att definiera expandergrafer.

Lemma 6.18. *Låt $\Gamma = (V, E, \mathrm{ep})$ vara en ändlig bipartit graf med uppdelning $V = V_0 \cup V_1$ och med uppåt begränsad valens $v \geq 1$. Antag även att $|V_0| = |V_1|$. Då gäller*

$$\frac{\check{h}(\Gamma) - 1}{2} \leq h(\Gamma) \leq v\check{h}(\Gamma).$$

Bevis. Vi börjar med att bevisa den högra olikheten. Välj godtyckligt $W \subset V_i$, $|W| \leq \frac{|V_i|}{2}$ för $i = 0$ eller $i = 1$. Från (2.12) vet vi att

$$\frac{|\partial W|}{|W|} \geq \frac{1}{v} \frac{|\mathcal{E}(W)|}{|W|} \geq \frac{1}{v} h(\Gamma).$$

vilket betyder att $v\check{h}(\Gamma) \geq h(\Gamma)$. För att bevisa den vänstra olikheten kan vi antaga att $\check{h}(\Gamma) \geq 1$. Detta är för att om $\check{h}(\Gamma) < 1$ så gäller olikheten trivialt. Sätt därför $\check{h}(\Gamma) = 1 + \delta$ där $\delta \geq 0$. Vi vill alltså visa att $h(\Gamma) \geq \frac{\delta}{2}$. Vi gör detta genom att välja godtyckligt $W \subset V$, $|W| \leq \frac{|V|}{2}$. Vi kan göra en uppdelning av noderna i W genom $W = W_0 \cup W_1$ där W_0 är de noder i W som ligger i V_0 och W_1 är de noder i W som ligger i V_1. Vi kan antag utan inskränkning att $|W_1| \leq |W_0|$. Eftersom W_1 och W_0 är disjunkta får vi att $|W| = |W_0| + |W_1| \leq 2|W_0|$ så att $|W_0| \geq \frac{|W|}{2}$. Vi kommer nu att dela upp i två fall beroende på storleken av $|W_0|$.

- ($|W_0| \leq \frac{|V_0|}{2}$) Från definitionen av $\check{h}(\Gamma)$ får vi

  $$1 + \delta = \check{h}(\Gamma) = \min(h_0, h_1) \leq h_0 = \min\left\{ \frac{|\partial W|}{|W|} \mid W \subset V_0, 1 \leq |W| \leq \frac{|V_0|}{2} \right\} \leq \frac{|\partial W_0|}{|W_0|}.$$

  så att $|\partial W_0| \geq (1 + \delta)|W_0|$. Antalet olika noder i ∂W_0 som ligger i V_1 men ej i W_1 ges av

  $$|\partial W_0| - |\partial W_0 \cap W_1| \geq (1 + \delta)|W_0| - |W_1| \geq (1 + \delta)|W_0| - |W_0| = \delta|W_0|.$$

  Eftersom $\delta|W_0| \geq \frac{\delta}{2}|W|$ får vi

  $$\frac{|\mathcal{E}(W)|}{|W|} \geq \frac{|\partial W|}{|W|} \geq \frac{\delta}{2}. \tag{23}$$

- ($|W_0| > \frac{|V_0|}{2}$) I detta fall vet vi att det finns en delmängd A till W_0 med storlek $\left\lceil \frac{|V_0|}{2} \right\rceil$. Vi kommer för enkelhetens skull anta att $|A| = \frac{|V_0|}{2}$. Vi har

  $$1 + \delta \leq \frac{|\partial A|}{|A|} \leq \frac{|\partial W_0|}{|V_0|/2}$$

så att $|\partial W_0| \geq (1+\delta)\frac{|V_0|}{2}$. Eftersom $|V| = |V_0| + |V_1|$ och $|V_0| = |V_1|$ får vi att $|W| = |W_0| + |W_1| \leq |V| = \frac{|V_0|}{2}$ och speciellt $|W_1| \leq \frac{|V_0|}{2}$. Antalet noder i ∂W_0 som ligger i V_1 men ej i W_1 ges av

$$|\partial W_0| - |\partial W_0 \cap W_1| \geq (1+\delta)\frac{|V_0|}{2} - |W_1| \geq (1+\delta)\frac{|V_0|}{2} - \frac{|V_0|}{2} = \delta\frac{|V_0|}{2} = \delta\frac{|V|}{4}.$$

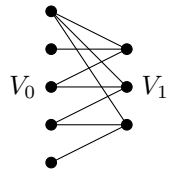
detta tillsammans med att $|W| \leq \frac{|V|}{2}$ ger oss att antalet noder i ∂W_0 som ligger i V_1 men ej i W_1 är minst $\delta\frac{|W|}{2}$. Vi får då att

$$\frac{|\mathcal{E}(W)|}{|W|} \geq \frac{|\partial W|}{|W|} \geq \frac{\delta}{2}. \tag{24}$$

Ekvation (23) tillsammans med (24) ger oss till slut att $h(\Gamma) \geq \frac{\delta}{2}$. □

Innan vi definierar expanderkoder kommer vi snabbt att gå över hur vi kommer att koppla bipartita grafer till paritetsmatriser. Vi låter V_0 ha lika många noder som antalet kolonner hos paritetsmatrisen och V_1 lika många noder som antalet rader hos paritetsmatrisen. En etta på plats (i, j) betyder då att det går en kant mellan en nod $i \in V_0$ till en nod $j \in V_1$. Till exempel fås grafen i Figur 2 från

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$



Figur 2: Ett exempel på en bipartit graf från en paritetsmatris.

Vi kan nu definiera expanderkoder.

Definition 6.19 (Expanderkod)**.** Om paritetsmatrisen för en linjär kod beskrivs av en bipartit expandergraf $\Gamma = (V, E, \text{ep})$ med uppdelning $V = V_0 \cup V_1$ där V_0 är k-reguljär sägs denna kod vara en expanderkod.

Det var Robert G. Gallager som vid 1969 först studerade detta sätt att skapa koder på genom att använda slumpmässiga glesa grafer. Detta utvecklades sedan vidare vid 1996 av Daniel A. Spielman som visade följande två satser [3].

Vi kommer att börja med att visa att en expanderkod har ett stort avstånd.

Sats 6.20 (Avstånd för expanderkoder)**.** *Låt $\Gamma = (V, E, \text{ep})$ vara en bipartit expandergraf med uppdelning $V = V_0 \cup V_1$ där V_0 är k-reguljär så att $h_0 > \frac{k}{2}$. För koden från denna graf gäller då*

$$d(C) > h_0|W| \tag{25}$$

där $W \subset V_0$ är mängden för vilken h_0 antar sitt minsta värde.

För att kunna fullborda satsen med dess bevis behöver vi först följande lemma.

Lemma 6.21. *Låt $\Gamma = (V, E, \text{ep})$ en bipartit expandergraf med uppdelning $V = V_0 \cup V_1$ så att V_0 är k-reguljär och $h_0 > \frac{k}{2}$. För varje delmängd $W \subseteq V_0$ existerar i så fall ett $y \in V_1$ så att*

$$\left|\partial\{y\} \cap W\right| = 1$$

Bevis. Antag att detta krav inte gäller för W. Då har varje $y \in \partial(W)$ minst två grannar som befinner sig i W. Antalet kanter som i så fall lämnar W är åtminstone

$$2\partial(W) > 2\frac{k}{2}|W| = k|W|\,.$$

Detta är en motsägelse eftersom V_0 är k-reguljär och antalet kanter som lämnar W egentligen är exakt $k|W|$. □

Med detta lemma framfört kan vi nu bevisa avstånd för expanderkoder.

Bevis. Vi antar att $d(C) \leq h_0|W|$. Enligt Lemma 6.15 existerar då ett nollskilt kodord ω vars vikt är som mest $h_0|W|$. Vi definierar mängden av noder där detta kodord har koordinater lika med ett, $X = \{i \mid \omega_i = 1\}$. Det finns enligt Lemma 6.21 då ett $y \in \partial(X)$. Denna nod y motsvarar en paritetssumma över ett kodord enligt konstruktion. Enligt definitionen för paritetsmatris skall denna summa dock vara noll och vi har en motsägelse. □

Förutom att expanderkoder har ett stort avstånd har dessa koder även en algoritm som kan avkoda på linjär tid. Denna går ut på att vid varje iteration singla en godtycklig koordinat som har majoriteten av dess bivillkor ouppfyllda. Då vi endast har två symboler att jobba med råder det inga tvivel om vilket värde man singlar till.

Sats 6.22 (Avkodning för expanderkoder)**.** *För en expanderkod med $h_0 > \frac{3k}{4}$ så avkodar en sådan algoritm det mottagna ordet v till det ursprungliga kodordet u efter ett linjärt antal iterationer om antalet fel är färre än $\frac{h_0|W|}{2}$ där $W \subset V_0$ är mängden för vilken h_0 antar sitt minsta värde.*

Bevis. Vi definierar felmängden $E = \{i \mid u_i \neq v_i\}$. Om denna är tom är vi klara, annars antar vi att $|E| \leq h_0|W|$. Vi delar upp mängden $\partial(E)$ i uppfyllda bivillkor S och ouppfyllda bivillkor U och noterar att

$$|S| + |U| = |\partial(E)| > \frac{3}{4}k|E|.$$

Vi noterar även att antalet kanter som går mellan E och $\partial(E)$ är som minst

$$|U| + 2|S| \leq k|E|.$$

Dessa olikheter ger tillsammans att

$$|U| > \frac{1}{2}k|E|. \tag{26}$$

Detta betyder alltså att så länge det finns ett fel finns det en koordinat i E som har fler än $\frac{k}{2}$ ouppfyllda bivillkor. Dessutom innebär detta då att algoritmen kommer att köra så länge det finns fel. Eftersom varje singling från början kommer att ha fler ouppfyllda bivillkor än uppfyllda kommer U att krympa.

Så länge $|E| \leq h_0|W|$ gäller kommer algoritmen att avbryta på kodordet närmast det mottagna ordet. Varje singling motsvarar att E minskar eller ökar med ett element. Men för att $|E|$ någonsin ska kunna överskrida denna gräns måste det finnas en felmängd E så att $|E| = h_0|W|$. I så fall måste $|U| > k\frac{h_0|W|}{2}$ enligt (26). Å andra sidan hade vi från antagandet om antalet fel att $|U| \leq k\frac{h_0|W|}{2}$ från början. □

A Linjär algebra

Definition A.1. Spåret av en kvadratisk matris är summan av dess diagonalelement. Om A är en kvadratisk matris så betecknar vi dess spår med Tr A.

Vi har

$$\text{Tr } AB = \sum_i \sum_j a_{ij} b_{ji} = \sum_j \sum_i b_{ji} a_{ij} = \text{Tr } BA.$$

Av detta följer att $\text{Tr}(T^{-1}AT) = \text{Tr}(TT^{-1}A) = \text{Tr } A$. Detta betyder att om A och A' är två matriser som representerar samma linjära avbildning i olika baser så är Tr $A =$ Tr A'. Alltså kan vi definiera spåret av en linjär avbildning som spåret av någon matris som representerar den.

Sats A.2 (Riesz representationssats)**.** *Låt H vara ett ändligtdimensionellt Hilbertrum. Om f är en linjär funktional på H så finns en unik vektor $v \in H$ så att $f(u) = \langle u, v\rangle$ för alla $u \in H$.*

Om A är en linjär operator på det ändligtdimensionella Hilbertrummet H och $v \in H$ så kan vi definiera en linjär funktional på H genom $u \mapsto \langle Au, v\rangle$. Enligt Riesz representationssats så finns då en unik vektor $A^*v \in H$ så att $\langle Au, v\rangle = \langle u, A^*v\rangle$. Avbildningen $v \mapsto A^*v$ definierar en linjär operator på H, som vi kallar för *adjugatet av A* och betecknar med A^*. Om vi skriver ner matrisen av A i en ortonormal bas så får vi matrisen av A^* i samma bas genom att ta det Hermiteska konjugatet av A (d.v.s. matrisenelementen av A^* är $\overline{a_{ji}}$ om matriselementen av A är a_{ij}).

Definition A.3. En linjär operator A på ett Hilbertrum H är *unitär* om $A^{-1} = A^*$.

Definition A.4. En linjär operator A på ett Hilbertrum H är *självadjungerande* om $\langle Au, v\rangle = \langle u, Av\rangle$ gäller för alla $u, v \in H$, det vill säga $A = A^*$.

Sats A.5. *Antag att A är en självadjungerande operator på ett Hilbertum H. Då är alla egenvärden till A reella, och egenvektorer hörande till olika egenvärden är ortogonala.*

Bevis. Antag att λ är ett egenvärde till A, och att $x \in H$ är en egenvektor hörande till λ. Vi har

$$\begin{aligned}(\lambda - \overline{\lambda})\langle x, x\rangle &= \lambda\langle x, x\rangle - \overline{\lambda}\langle x, x\rangle \\ &= \langle \lambda x, x\rangle - \langle x, \lambda x\rangle \\ &= \langle Ax, x\rangle - \langle x, Ax\rangle = 0.\end{aligned}$$

Eftersom $\langle x, x\rangle \neq 0$ så måste $\lambda = \overline{\lambda}$, vilket visar att λ är ett reellt tal.

Antag nu att $\mu \neq \lambda$ är ett annat egenvärde till A, och att $y \in H$ är en egenvektor hörande till μ. På samma sätt som innan har vi

$$(\lambda - \mu)\langle x, y\rangle = \langle Ax, y\rangle - \langle x, Ay\rangle = 0.$$

Eftersom $\lambda \neq \mu$ så måste $\langle x, y\rangle = 0$. Alltså är x och y ortogonala mot varandra. □

Sats A.6. *Om A är en självadjungerande operator på ett ändligtdimensionellt Hilbertrum H så har A en ortonormal egenbas.*

Bevis. Vi bevisar satsen genom induktion på dimensionen av H. Påståendet är uppenbarligen sant om $\dim H = 1$. Antag nu att påståendet är sant för alla Hilbertrum av dimension lägre än n, och att $\dim H = n$. Låt λ vara ett egenvärde till A och låt u vara en egenvektor hörande till λ. Låt $U = \langle v\rangle^\perp$. Då är $H = U \oplus \langle u\rangle$. Eftersom A är självadjungerad så följer det att U är ett invariant delrum. Eftersom $\dim U < n$ så finns enligt induktionsantagandet en ortonormal egenbas $\mathcal{B}$ till A begränsad till U. Låter vi $e \in \langle v\rangle$ vara en normerad vektor så är $\mathcal{B} \cup \{e\}$ en ortonormal egenbas till A. □

Lemma A.7. *Om A och B är kommuterande operatorer så är varje egenrum till A ett invariant delrum till B.*

Bevis. Låt λ vara ett egenvärde till A, och u en egenvektor hörande till λ. Vi har då $\lambda Bu = BAu = ABu$, vilket visar att Bu är en egenvektor hörande till λ. □

Definition A.8. En operator A på ett Hilbertrum är *normal* om $AA^* = A^*A$.

Sats A.9. *Om A är en normal operator på ett ändligtdimensionell Hilbertrum H så har A en ortonormal egenbas.*

Bevis. Skriv $A = B+iC$, där $B = \frac{A+A^*}{2}$ och $C = \frac{A-A^*}{2i}$. Då är B och C självadjungerande. En enkel uträkning visar att $BC = CB$. Det följer av sats (A.6) att vi kan skriva $H = \mathcal{E}(\lambda_1)\oplus\cdots\oplus\mathcal{E}(\lambda_k)$, där $\mathcal{E}(\lambda_i)$ är egenrummen till B. Eftersom varje $\mathcal{E}(\lambda_i)$ är invariant under C, och C är diagonaliserbar, så kan vi hitta en ortonormal egenbas $\mathcal{B}_i$ till $C|_{\mathcal{E}(\lambda_i)}$ för varje i. Då är $\mathcal{B} = \bigcup_i \mathcal{B}_i$ en ortonormal bas som är en egenbas både för B och C. Eftersom $A = B + iC$ så följer det att $\mathcal{B}$ är en ortonormal egenbas för A. □

Korollarium A.10. *En unitär operator A på ett ändligtdimensionellt Hilbertrum H har en ortonormal egenbas.*

Bevis. Vi har $AA^* = AA^{-1} = I = A^{-1}A = A^*A$. Alltså är A normal, och påståendet följer från Sats A.9. □

Sats A.11. *Antag att A är en självadjungerande operator på ett ändligtdimensionellt Hilbertrum H. Det minsta egenvärdet till A är då lika med*

$$\min_{0\neq x\in H} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}.$$

Bevis. Låt $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$ vara egenvärdena till A. Enligt Spektralsatsen (A.9) så finns det en ortonormal bas $e_1, e_2, \ldots, e_n$ av H så att $Ae_i = \lambda_i$ för $i = 1, 2, \ldots, n$. Om $x = \sum_{i=1}^n x_i e_i$ så har vi

$$\frac{\langle Ax, x\rangle}{\langle x, x\rangle} = \frac{\sum_{i=1}^n \lambda_i |x_i|^2}{\sum_{i=1}^n |x_i|^2}.$$

Detta uttrycket är större än eller lika med λ_1, och vi får likhet om vi stoppar in $x = e_1$. Av detta följer satsen. □

B Representationsteori

Definition B.1. En homomorfi $\varphi : G \to GL(V)$ kallas en linjär representation av gruppen G. Om $\dim V = n$ sägs φ vara n-dimensionell, eller vara av grad n. Vidare gör vi följande defintioner:

(1) Ett underrum U till V sägs vara G-invariant om $\varphi(g)U = U$ för alla $g \in G$.

(2) Om det inte finns något äkta och icketrivialt G-invariant underrum till V, kallas φ irreducibel.

(3) Om $\varphi(g)$ är unitär för alla $g \in G$, kallas φ unitär.

(4) Om $\varphi(g) = I$ för alla $g \in G$, kallas φ trivial.

Samtliga representationer vi betraktar är linjära. I fortsättningen betonar vi därför inte detta, och talar enbart om *representationer*.

Definition B.2 (Den reguljära representationen)**.** Representationen $\pi : G \to GL(L^2(G))$ som definieras genom

$$\pi_g f(x) = f(g^{-1}x),$$

kallas för den reguljära representationen.

Lemma B.3. *Den reguljära representationen π av en grupp G är en unitär representation.*

Bevis. Låt $f, h \in L^2(G)$. För ett godtyckligt $g \in G$ är

$$\begin{aligned}\langle \pi_g(f), \pi_g(h) \rangle &= \frac{1}{|G|} \sum_{x \in G} f(g^{-1}x)\overline{h(g^{-1}x)} \\ &= \frac{1}{|G|} \sum_{x' \in G} f(x')\overline{h(x')} \\ &= \langle f, h \rangle,\end{aligned}$$

där den näst sista likheten följer av att $gG = G$ för alla $g \in G$. □

Avslutningsvis noterar vi att funktionerna δ_x som defineras av

$$\delta_x(g) = \begin{cases} 1, & g = x \\ 0, & g \neq x \end{cases}$$

bildar en bas i $L^2(G)$.

C Fouriertransform på $(\mathbb{Z}/n\mathbb{Z})^2$

Möjligheten att kunna fouriertransformera funktioner i $L^2(G)$, vektorrummet av alla funktioner på en grupp G, ger ett kraftfullt verktyg till att studera funktioner definierade på en grupp. I $L^2(G)$ definierar vi en inre produkt genom

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

Vi kan nu notera att denna skalärprodukt överensstämmer med skalärprodukten av funktioner definierade på en reguljär graf Γ vara noder är elementen i G, se Ekvation (6). Detta innebär att vi inte behöver göra någon skillnad mellan $L^2(\Gamma)$ och $L^2(G)$ när det gäller fouriertransform av funktioner som ligger i dessa vektorrum.

I fortsättningen av detta avsnitt låter vi G vara den abelska gruppen $(\mathbb{Z}/n\mathbb{Z})^2$. Speciellt gäller det då att $|G| = n^2$. I detta fall då G är en abelsk grupp visar det sig att fouriertransformen blir speciellt enkel.

Definition C.1. Fouriertransformen är en linjär avbildning

$$\begin{cases} L^2(G) \to L^2(G) \\ f \to \hat{f} \end{cases}$$

definierat som

$$\hat{f}(\mu) = \langle f, \chi_\mu \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\chi_\mu(x)}$$

där $\chi_\mu(x) = e^{2\pi i \frac{\mu \cdot x}{n}}$ är de så kallade karaktärerna för G.

Med $\cdot$ menar vi den vanliga skalärprodukten i $\mathbb{R}^2$. En viktig egenskap för $\{\chi_\mu\}_{\mu \in G}$ är att de utgör en ON-bas för $L^2(G)$. Detta inses genom att notera att $\dim(L^2(G)) = |G|$ och beräkna

$$\langle \chi_a, \chi_b \rangle = \frac{1}{|G|} \sum_{x \in G} \chi_a(x)\overline{\chi_b(x)} = \frac{1}{|G|} \sum_{x_1=0}^{n-1} \sum_{x_2=0}^{n-1} e^{2\pi i \frac{(a-b)\cdot x}{n}} = \begin{cases} 1, & a = b \\ 0, & a \neq b \end{cases}$$

där den sista likheten fås genom att observera att den inre summan är en geometrisk serie. Utifrån detta kan man då för varje $f \in L^2(G)$ skriva

$$f(x) = \sum_{\mu \in G} \langle f, \chi_\mu \rangle \chi_\mu(x) = \sum_{\mu \in G} \hat{f}(\mu)\chi_\mu(x).$$

Denna formel för f kallar vi för inversionsformeln.

Proposition C.2 (Plancherels sats)**.** *För $f, g \in L^2(G)$ gäller det att $\langle f, g\rangle = |G|\langle \hat{f}, \hat{g}\rangle$*

Bevis. Genom att använda definitionen av fouriertransform tillsammans med inversionsformeln får vi

$$\begin{aligned}\langle f, g\rangle &= \frac{1}{|G|}\sum_{y\in G} f(y)\overline{g(y)} = \frac{1}{|G|}\sum_{y,\mu\in G} f(y)\overline{\hat{g}(\mu)\chi_\mu(y)} \\ &= \sum_{\mu\in G}\overline{\hat{g}(\mu)}\frac{1}{|G|}\sum_{y\in G} f(y)\overline{\chi_\mu(y)} = \sum_{\mu\in G}\overline{\hat{g}(\mu)}\hat{f}(\mu) = |G|\langle \hat{f}, \hat{g}\rangle.\end{aligned}$$

□

Vi kommer nu att undersöka några räkneregler för fouriertransformen av funktioner i $L^2(G)$. Låt $f \in L^2(G)$, $A \in GL(2, \mathbb{Z}/n\mathbb{Z})$ och $\psi(x) = f(Ax)$, då är

$$\begin{aligned}\hat{\psi}(\mu) &= \frac{1}{|G|}\sum_{x\in G}\psi(x)e^{-2\pi i\frac{\mu\cdot x}{n}} \\ &= \frac{1}{|G|}\sum_{x\in G} f(Ax)e^{-2\pi i\frac{\mu\cdot x}{n}} \\ &= \frac{1}{|G|}\sum_{x'\in G} f(x')e^{-2\pi i\frac{\mu\cdot A^{-1}x'}{n}}\end{aligned}$$

Vi ser att

$$\mu\cdot A^{-1}x' = \mu^T A^{-1}x' = ((A^{-1})^T\mu)^T x' = (A^{-1})^T\mu\cdot x',$$

så

$$\hat{\psi}(\mu) = \hat{f}((A^{-1})^T\mu). \tag{27}$$

Om istället $\psi(x) = f(x + a)$, så är

$$\begin{aligned}\hat{\psi}(\mu) &= \frac{1}{|G|}\sum_{x\in G}\psi(x)e^{-2\pi i\frac{\mu\cdot x}{n}} \\ &= \frac{1}{|G|}\sum_{x\in G} f(x+a)e^{-2\pi i\frac{\mu\cdot x}{n}} \\ &= \frac{1}{|G|}\sum_{x'\in G} f(x')e^{-2\pi i\frac{\mu\cdot(x'-a)}{n}} \\ &= \chi_\mu(a)\hat{f}(\mu).\end{aligned} \tag{28}$$

Det följer nu av Ekvation (27) och Ekvation (28) att om $\psi(x) = f(Ax + a)$, så är

$$\hat{\psi}(\mu) = \chi_\mu(a)\hat{f}((A^{-1})^T\mu). \tag{29}$$

D Gruppen $SL(2, \mathbb{F}_p)$

I detta avsnitt ska vi studera ett par viktiga egenskaper hos den *speciella linjära gruppen* $SL(2, \mathbb{F}_p)$ där $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ för ett primtal p. Denna grupp består av alla 2×2-matriser med determinant 1 och koefficienter i $\mathbb{F}_p$, nämligen

$$SL(2, \mathbb{F}_p) = \left\{ \begin{bmatrix} a & b \\ c & d\end{bmatrix} \mid a, b, c, d \in \mathbb{F}_p \text{ och } ad - bc = 1 \right\}.$$

Två element i $SL(2, \mathbb{F}_p)$ multipliceras enligt vanlig matrismultiplikation med tillägget att man måste lägga till eller dra ifrån multipler av p så att koefficienterna ligger i $\mathbb{F}_p$. Om till exempel $p = 5$ får vi att

$$\begin{bmatrix} 2 & 0 \\ 0 & 3\end{bmatrix}\begin{bmatrix} 1 & 1 \\ 2 & 3\end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 4\end{bmatrix} \in SL(2, \mathbb{F}_5)$$

och

$$\begin{bmatrix} 2 & 2 \\ 1 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 4 & -2 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 4 & 2 \end{bmatrix} \in SL(2, \mathbb{F}_5).$$

Storleken av $SL(2, \mathbb{F}_p)$ kan bestämmas genom att studera den närbesläktade gruppen $GL(2, \mathbb{F}_p)$ som består av alla 2×2-matriser med nollskild determinant och koefficienter i $\mathbb{F}_p$. Determinanten kan man se som en homomorfi från $GL(2, \mathbb{F}_p)$ till den multiplikativa gruppen $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ av $\mathbb{F}_p$. Denna observation tillsammans med att kärnan till determinantfunktionen är $SL(2, \mathbb{F}_p)$ gör att vi kan bestämma storleken av $SL(2, \mathbb{F}_p)$

Proposition D.1. $|SL(2, \mathbb{F}_p)| = p(p^2 - 1)$.

Bevis. Determinantfunktionen $\det : GL(2, \mathbb{F}_p) \to \{1, 2, \ldots, p-1\} = \mathbb{F}_p^*$ är en homomorfi eftersom determninanten är multiplikativ. Vidare är denna homomorfi surjektiv eftersom för $a \in \mathbb{F}_p^*$ är

$$\det \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = a.$$

Kärnan till denna homomorfi, det vill säga de matriser som avbildas på enheten i $\mathbb{F}_p^*$, är $SL(2, \mathbb{F}_p)$. Första isomorfismsatsen säger då att $GL(2, \mathbb{F}_p)/SL(2, \mathbb{F}_p) \cong \mathbb{F}_p^*$ vilket ger oss

$$|SL(2, \mathbb{F}_p)| = \frac{|GL(2, \mathbb{F}_p)|}{|\mathbb{F}_p^*|} = \frac{|GL(2, \mathbb{F}_p)|}{p-1}$$

Det återstår nu att bestämma storleken av $GL(2, \mathbb{F}_p)$. Detta gör vi genom ett enkelt kombinatoriskt argument. Antalet möjliga alternativ för den första raden är $(p^2 - 1)$. Detta är för att det totala antalet alternativ för den första raden är p^2 men för att få en inverterbar matris måste vi ta bort det alternativ som matsvarar en nollrad. Antalet alternativ för den andra raden blir därefter $(p^2 - p)$. Detta är för att vi från det totala antalet alternativ för den andra raden, p^2, tar bort alla multiplar av den första raden. Genom att göra detta blir raderna linjärt oberoende och motsvarande matris inverterbar. Vi får då att

$$|GL(2, \mathbb{F}_p| = (p^2 - 1)(p^2 - p) = p(p^2 - 1)(p - 1)$$

och därmed är $|SL(2, \mathbb{F}_p)| = p(p^2 - 1)$. □

Proposition D.2. *De två matriserna*

$$T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \textit{och} \quad T_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

genererar $SL(2, \mathbb{F}_p)$.

Bevis. Eftersom

$$T_1^x = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad \text{och} \quad T_2^y = \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix}$$

räcker det att visa att matriser av formen T_1^x och T_2^y där $x, y \in \mathbb{F}_p$ genererar $SL(2, \mathbb{F}_p)$. Vi gör detta genom att dela upp i olika fall. Om $b \neq 0$ kan vi skriva

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{d-1}{b} & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{a-1}{b} & 1 \end{bmatrix}.$$

Om $c \neq 0$ kan vi skriva

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & \frac{a-1}{c} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{bmatrix}$$

Om $b = 0$ och $c = 0$ är $a \neq 0$ och vi kan skriva vår matris som

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{1-a}{a} & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{-1}{a} \\ 0 & 1 \end{bmatrix}$$

I samtliga fall har vi skrivit ett element i $SL(2, \mathbb{F}_p)$ som en produkt av element av den önskade formen. □

E Probabilistiskt bevis av expandergrafers existens

Vi visar här att expandergrafer existerar genom att betrakta en reguljär bipartit graf där kanterna väljs slumpmässigt. Beviset följer i fotspåren av [4].

Låt $n \geq 2$ och $k \geq 3$, och låt $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_k)$ vara likformigt och slumpmässigt vald ur S_n^k, där S_n är mängden av alla bijektioner från $\{1, \dots, n\}$ till sig själv. Vi definierar först en bipartit graf $\Gamma_{\boldsymbol{\sigma}}^{(n)} = (V_n, E_n, \text{ep})$ med hörnen $V_n = V_0 \cup V_1$, där

$$V_0 = \{(i, 0) : 1 \leq i \leq n\}, \quad V_1 = \{(i, 1) : 1 \leq i \leq n\}.$$

Kanterna definieras sedan enligt

$$E_n = \{(i, \sigma_j(i)) : 1 \leq i \leq n, 1 \leq j \leq k\},$$

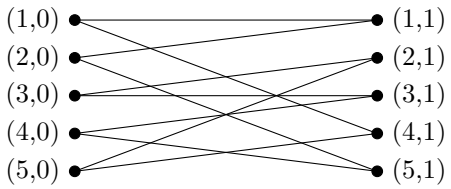
och ändpunktsfunktionen tas till att vara

$$\text{ep}((i, \sigma_j(i))) = \{(i, 0), (\sigma_j(i), 1)\}.$$

Notera att alla hörn i V_0 har grad k per konstruktion, och att alla hörn i V_1 också har grad k eftersom varje σ_j är en bijektion. Alltså är grafen k-reguljär. Ett exempel på hur grafen ser ut då $n = 5$ och $k = 2$, med permutationerna $(1452)(3)$ och $(1)(2543)$ visas i Figur 3.

Eftersom $\boldsymbol{\sigma}$ är likformigt slumpmässigt vald är

$$P(\Gamma_{\boldsymbol{\sigma}}^{(n)} \text{ har egenskap } \mathcal{P}) = \frac{|\{\boldsymbol{\sigma} : \Gamma_{\boldsymbol{\sigma}}^{(n)} \text{ har egenskap } \mathcal{P}\}|}{|S_n|^k}.$$



Figur 3: Ett exempel på hur en av graferna i familjen ser ut, då $n = 5$ och $k = 2$, med permutationerna $(1452)(3)$ och $(1)(2543)$.

Sats E.1. *Låt $k \geq 3$ vara fix. Det existerar ett $h_k > 0$ sådant att*

$$\lim_{n \to \infty} P(h(\Gamma_{\boldsymbol{\sigma}}^{(n)}) < h_k) = 0. \tag{30}$$

Definition E.2 (Grafavbildning, Grafisomorfism)**.** Låt Γ_1 och Γ_2 vara grafer. Ett par (f, f_*), där $f : V_{\Gamma_1} \to V_{\Gamma_2}$ och $f_* : E_{\Gamma_1} \to E_{\Gamma_2}$, kallas en grafavbildning om $f(\text{ep}(\alpha)) = \text{ep}(f_*(\alpha))$ för alla $\alpha \in E_{\Gamma_1}$. Om f och f_* är bijektiva kallas (f, f_*) en grafisomorfism från Γ_1 till Γ_2.

Lemma E.3. *Låt Γ_1 och Γ_2 vara grafer, och antag att det finns en grafisomorfism (f, f_*) från Γ_1 till Γ_2. Då är $|\partial W| = |\partial f(W)|$ för alla $W \subset V_{\Gamma_1}$.*

Bevis. Låt $w_i \in W$, och låt A_i vara mängden av alla grannar till w_i som inte ligger i W. Notera att $f(\cup_i A_i) = \cup_i f(A_i)$. Eftersom f är en bijektion blir då $|\partial W| = |\cup_i A_i| = |f(\cup_i A_i)| = |\cup_i f(A_i)|$. Med villkoret för grafavbildningar kan vi visa att $f(A_i)$ är mängden av alla grannar till $f(w_i)$ som inte ligger i $f(W)$, vilket ger att $|\partial f(W)| = |\cup_i f(A_i)| = |\partial W|$. □

Bevis av Sats E.1. Av Lemma (6.18) följer att

$$P(h(\Gamma_{\boldsymbol{\sigma}}^{(n)}) < h_k) \leq P(\check{h}(\Gamma_{\boldsymbol{\sigma}}^{(n)}) < 2h_k + 1).$$

Låt $\delta = 2h_k$, och beteckna sannolikheten i vänsterledet med p_n. Enligt Definition 6.17 har vi att $\check{h}(\Gamma_{\boldsymbol{\sigma}}^{(n)}) = \min(h_0(\Gamma_{\boldsymbol{\sigma}}^{(n)}), h_1(\Gamma_{\boldsymbol{\sigma}}^{(n)}))$, och ytterligare en överskattning ger att

$$p_n \leq P(h_0(\Gamma_{\boldsymbol{\sigma}}^{(n)}) < \delta + 1) + P(h_1(\Gamma_{\boldsymbol{\sigma}}^{(n)}) < \delta + 1).$$

Notera att $E_n = \{(i, \sigma_j(i)) : 1 \leq i \leq n, 1 \leq j \leq k\} = \{(\sigma_j^{-1}(i), i) : 1 \leq i \leq n, 1 \leq j \leq k\}$, så att $h_1(\Gamma_{\boldsymbol{\sigma}}^{(n)}) = h_0(\Gamma_{\boldsymbol{\sigma}^{-1}}^{(n)})$. Men eftersom $(S_n^k)^{-1} = S_n^k$, fås följaktligen att

$$p_n \leq 2P(h_0 < \delta + 1) \leq 2 \sum_{\substack{W \subset V_0 \\ |W| \leq \frac{1}{2}V_0}} P(|\partial_{\boldsymbol{\sigma}} W| < (\delta + 1)|W|), \tag{31}$$

där vi i den andra olikheten har utnyttjat att $P(h_0 < \delta + 1)$ inkluderas i summan.

Låt nu $W \subset V_0$ med $|W| = \ell \leq \frac{n}{2}$, och lista hörnen i V_0 enligt

$$(x_1, 0), (x_2, 0), \ldots, (x_\ell, 0), (x_{\ell+1}, 0), \ldots, (x_n, 0),$$

där $W = \{(x_1, 0), (x_2, 0), \ldots, (x_\ell, 0)\}$. Lista också hörnen i V_1 på motsvarande vis. Definiera funktionen $g : \mathbb{N}_n \to \mathbb{N}_n$ enligt $g(x_i) = i$, vilken har en invers $g^{-1}(i) = x_i$. Paret (f, f_*) med f och f_* definierade enligt

$$\begin{cases} f((x,0)) = (g(x), 0), \quad f((x,1)) = (g(x), 1) \\ f_*((x, \sigma_j(x))) = (g(x), g(\sigma_j(x))) \end{cases}$$

kan visas vara en grafavbildning. Notera att f och f_* är bijektiva, ty de har inverserna

$$\begin{cases} f^{-1}((x,0)) = (g^{-1}(x), 0), \quad f^{-1}((x,1)) = (g^{-1}(x), 1) \\ f_*^{-1}((x, \sigma_j(x))) = (g^{-1}(x), g^{-1}(\sigma_j(x))) \end{cases}$$

Alltså är (f, f_*) en grafismorfism. Eftersom $f(W) = \{(1,0), \ldots, (\ell, 0)\}$ följer enligt Lemma E.3 att Ekvation (31) är ekvivalent med

$$p_n \leq 2 \sum_{1 \leq \ell \leq \frac{n}{2}} \binom{n}{\ell} P(|\partial_{\boldsymbol{\sigma}} \{(1,0), \ldots, (\ell, 0)\}| < (\delta + 1)\ell). \tag{32}$$

Om vi nu låter endast den första permutationen, σ_1, i $\boldsymbol{\sigma}$ verka på $\{(1,0), \ldots, (\ell, 0)\}$ får vi mängden $I_\ell \subseteq V_1$ med storlek ℓ eftersom σ_1 är en bijektion. Detta innebär att

$$\begin{aligned} &P(|\partial_{\boldsymbol{\sigma}} \{(1,0), \ldots, (\ell, 0)\}| < (\delta + 1)\ell) \\ =\ &P(|(\partial_{\boldsymbol{\sigma} \setminus \sigma_1} \{(1,0), \ldots, (\ell, 0)\}) \setminus I_\ell| < \delta\ell) \\ \leq\ &P(|(\partial_{\boldsymbol{\sigma} \setminus \sigma_1} \{(1,0), \ldots, (\ell, 0)\}) \setminus I_\ell| \leq \lfloor \delta\ell \rfloor) \\ \leq\ &P(|(\partial_{\sigma_2 \cup \sigma_3} \{(1,0), \ldots, (\ell, 0)\}) \setminus I_\ell| \leq \lfloor \delta\ell \rfloor), \end{aligned}$$

där den sista olikheten följer av att om $(\sigma_2, \ldots, \sigma_k)$ verkar på $\{(1,0), \ldots, (\ell, 0)\}$ och avbildas på som mest $\lfloor \delta\ell \rfloor$ element utanför I_ℓ så måste endast σ_2 och σ_3 tillsammans avbildas på som mest $\lfloor \delta\ell \rfloor$ element utanför I_ℓ. Dessutom, att σ_2 och σ_3 avbildas på som mest $\lfloor \delta\ell \rfloor$ element utanför I_ℓ implicerar att $A \subseteq (I_\ell \cup E)$ för någon E som är en delmängd i $V_1 \setminus I_\ell$, där $A = (\partial_{\sigma_2 \cup \sigma_3} \{(1,0), \ldots, (\ell, 0)\})$. Vi

får då att

$$\begin{aligned}
&P(|(\partial_{\sigma_2\cup\sigma_3}\{(1,0),\dots,(\ell,0)\})\backslash I_\ell| \le \lfloor \delta\ell \rfloor) \\
\le& P(\bigcup_{|E|=\lfloor\delta\ell\rfloor} (A \subseteq (I_\ell \cup E))) \\
\le& \sum_{|E|=\lfloor\delta\ell\rfloor} P(A \subseteq (I_\ell \cup E)) \\
=& \sum_{|E|=\lfloor\delta\ell\rfloor} P((\partial_{\sigma_2}\{(1,0),\dots,(\ell,0)\}) \subseteq (I_\ell \cup E))^2 \\
=& \binom{n-\ell}{\lfloor\delta\ell\rfloor} P((\partial_{\sigma_2}\{(1,0),\dots,(\ell,0)\}) \subseteq (I_\ell \cup E_\ell))^2 \\
\le& \binom{n}{\lfloor\delta\ell\rfloor} P((\partial_{\sigma_2}\{(1,0),\dots,(\ell,0)\}) \subseteq (I_\ell \cup E_\ell))^2
\end{aligned}$$

där E_ℓ är en fixerad delmängd av V_1 med storlek $\lfloor\delta\ell\rfloor$ som är disjunkt med I_ℓ. I den tredje och fjärde likheten har vi använt symmetri och att σ_2 och σ_3 är oberoende av varandra. Eftersom σ_2 är en bijektion gäller det att

$$\begin{aligned}
P((\partial_{\sigma_2}\{(1,0),\dots,(\ell,0)\}) \subseteq (I_\ell \cup E_\ell)) &= \frac{\ell+\lfloor\delta\ell\rfloor}{n} \cdot \frac{\ell+\lfloor\delta\ell\rfloor-1}{n-1} \cdots \frac{1+\lfloor\delta\ell\rfloor}{n-\ell+1} \\
&= \frac{(\ell+\lfloor\delta\ell\rfloor)!}{(\lfloor\delta\ell\rfloor)!}\frac{(n-\ell)!}{n!}.
\end{aligned}$$

Vi får då tillslut att

$$p_n \le 2\sum_{1\le\ell\le\frac{n}{2}} \binom{n}{\ell}\binom{n}{\lfloor\delta\ell\rfloor}\left(\frac{(\ell+\lfloor\delta\ell\rfloor)!}{(\lfloor\delta\ell\rfloor)!}\right)^2\left(\frac{(n-\ell)!}{n!}\right)^2 = 2\sum_{1\le\ell\le\frac{n}{2}} \frac{(n-\ell)!((\ell+\lfloor\delta\ell\rfloor)!)^2}{\ell!(n-\lfloor\delta\ell\rfloor)!(\lfloor\delta\ell\rfloor!)^3} \qquad (33)$$

Resterande del av beviset går ut på att visa att ovanstående summa går mot noll. Detta gör vi genom att dela upp summan i två serier vid $m_n = \ln(\ln(n))$, som ska vara stort, så att

$$\lim_{n\to\infty} S_n = \lim_{n\to\infty}(\sum_{\ell=1}^{m_n} a_\ell + \sum_{\ell=m_n+1}^{n/2} a_\ell).$$

I den första av dessa summor uppskattar vi termerna uppåt som

$$a_\ell \le \frac{((2\ell)!)^2}{(n-\lfloor\delta\ell\rfloor)\dots(n-\ell+1)} \le \frac{((2m_n)!)^2}{n} \le \frac{e^2(2m_n)^{4m_n+1}e^{-4m_n}}{n}$$

där vi använt att $n! \le e\cdot n^{n+1/2}e^{-n}$ för alla positiva n. Detta ger oss

$$\sum_{\ell=1}^{m_n} a_\ell \le \frac{m_n e^2(2m_n)^{4m_n+1}e^{-4m_n}}{n}.$$

Vi visar att ovanstående uttryck går mot noll då n går mot oändligheten genom att visa att dess logaritm går mot minus oändligheten.

$$\ln\left(\frac{m_n e^2(2m_n)^{4m_n+1}e^{-4m_n}}{n}\right) = \ln(m_n)+2+(4m_n+1)\ln(2m_n)-4m_n-\ln(n) \to -\infty \text{ då } n\to\infty.$$

Det återstår nu att visa att den andra summan går mot 0. Vi undersöker logaritmen av dess termer och använder att $\ln(k!) \approx k\ln(k)$ för stort k. Detta ger oss följande form för termernas logaritmer:

$$\ln(a_\ell) = (n-\ell)\ln(n-\ell) + 2(\ell+\delta\ell)\ln(\ell+\delta\ell) - \ell\ln(\ell) - (n-\delta\ell)\ln(n-\delta\ell) - 3\delta\ell\ln(\delta\ell), \quad (34)$$

där vi gjort approximationen $\lfloor \delta\ell \rfloor \approx \delta\ell$. Den första och fjärde termen i (34) blir

$$\begin{aligned}(n-\ell)\ln(n-\ell) - (n-\delta\ell)\ln(n-\delta\ell) &= n\ln(n-\ell) - \ell\ln(n-\ell) - n\ln(n-\delta\ell) + \delta\ell\ln(n-\delta\ell) \\ &= n\ln(1-\frac{\ell}{n}) - \ell\ln(1-\frac{\ell}{n}) - n\ln(1-\frac{\delta\ell}{n}) \\ &+ \delta\ell\ln(1-\frac{\delta\ell}{n}) + \ell(\delta-1)\ln(n) \\ &\leq (n-\ell)\ln(1-\frac{\ell}{n}) - (n-\ell)\ln(1-\frac{\delta\ell}{n}) + \ell(\delta-1)\ln(n) \\ &= \ell(\frac{n}{\ell}-1)\ln\left(\frac{1-\frac{\ell}{n}}{1-\frac{\delta\ell}{n}}\right) + \ell(\delta-1)\ln(n)\end{aligned}$$

där vi i den första likheten faktoriserat ut n från varje logaritm och vid den första olikheten använt att $\delta \leq 1$. Genom att sätta $\frac{\ell}{n} = x$ där $x \in (0, \frac{1}{2}]$ och göra en plot ser man lätt att följande olikhet gäller för små δ

$$(\frac{n}{\ell}-1)\ln\left(\frac{1-\frac{\ell}{n}}{1-\frac{\delta\ell}{n}}\right) \leq (\delta-1).$$

Detta ger oss tillslut att den första och fjärde termen i (34) begränsas uppåt av $(\delta-1)\ell + \ell(\delta-1)\ln(n)$. Genom att använda att $\ln(1+\delta) \leq \delta$ kan vi uppskatta den andra, tredje och femte termen i (34) som

$$2(\ell+\delta\ell)\ln(\ell+\delta\ell) - \ell\ln(\ell) - 3\delta\ell\ln(\delta\ell) \leq (2(1+\delta)\delta - 3\delta\ln(\delta))\ell + \ell(1-\delta)\ln(\ell),$$

vilket då ger oss följande uppskattning för logaritmen av a_ℓ:

$$\ln(a_\ell) \leq (2(1+\delta)\delta - 3\delta\ln(\delta) + \delta - 1)\ell + \ell(\delta-1)\ln\left(\frac{n}{\ell}\right) \leq c\ell + \ell(\delta-1)\ln(2)$$

där $c = (2(1+\delta)\delta - 3\delta\ln(\delta) + \delta - 1)$. Eftersom $(c + (\delta-1)\ln(2)) = -\beta$ är negativ för små δ gäller det att

$$\sum_{\ell=m_n+1}^{n/2} a_\ell \leq \sum_{\ell=m_n+1}^{n/2} e^{-\ell\beta} = e^{-\beta(m_n+1)}\frac{e^{-\beta(n/2-m_n)}-1}{e^{-\beta}-1} \to 0 \text{ då } n \to \infty.$$

vilket bevisar Sats 4.1 □

Sats 4.1 säger att det för varje tillräckligt stort n finns ett $\boldsymbol{\sigma} \in S_n^k$ så att $h(\Gamma_{\boldsymbol{\sigma}}^{(n)}) \geq h_k$. Detta tillsammans med att graferna $\Gamma_{\boldsymbol{\sigma}}^{(n)}$ är k-reguljära för alla n implicerar att expandergrafer måste existera.

F Litteraturförteckning

[1] Ya.M. Barzdin A.N. Kolmogorov. *On the realization of networks in three-dimensional space.*

[2] M. S. Pinsker. On the complexity of a concentrator, 7th International Teletraffic Conference, 1973, sida 138/1-138/4.

[3] A. Wigderson N. Linial. Expander graphs and their applications, 2001 jan. 1 [Besökt 2018 maj 9]. Tillgänglig från: `http://www.math.ias.edu/~boaz/ExpanderCourse/allnotes.pdf`.

[4] E. Kowalski. An introduction to expander graphs, 2017 nov. 25 [Besökt 2018 maj 9]. Tillgänglig från: `https://people.math.ethz.ch/~kowalski/expander-graphs.pdf`.

[5] V. Guruswami. Introduction to coding theory, 2010 [Besökt 2018 maj 9]. Tillgänglig från: `https://www.cs.cmu.edu/~venkatg/teaching/codingtheory/`.

[6] H. A. Helfgott. Growth in groups: ideas and perspectives, 2015 feb. 11. [Besökt 2018 maj 9]. Tillgänglig från: `http://www.ams.org/journals/bull/2015-52-03/S0273-0979-2015-01475-8/S0273-0979-2015-01475-8.pdf`.